

**From:** [Joseph McClelland](#)  
**To:** (b) (6)  
**Cc:** [David Andrejcek](#)  
**Subject:** FW: EMP COMMISSION REPORTS  
**Date:** Wednesday, May 09, 2018 4:56:00 AM  
**Attachments:** [Executive Report on Assessing the Threat from EMP - FINAL April2018.pdf](#)  
[Recommended E3 Waveform for Critical Infrastructures - FINAL April2018.pdf](#)  
[Life Without Electricity - FINAL April2018.pdf](#)  
[EMP Commission Vol1 Summary.pdf](#)  
[EMP COMM. RPT. CRIT. NAT. INFRASTRUCTURES.pdf](#)

---

**From:** Peter Pry [mailto:peterpry@verizon.net]

**Sent:** Wednesday, May 09, 2018 12:33 AM

**To:** Joseph McClelland <Joseph.McClelland@ferc.gov>

**Subject:** EMP COMMISSION REPORTS

Attached find the 3 unclassified 2018 EMP Commission reports and the two unclassified 2004 and 2008 EMP Commission Reports. 7 more EMP Commission reports, submitted to DOD unclassified that were supposed to be published in December 2017, still undergoing review (or being stalled) by DOD.--Peter

Dr. Peter Vincent Pry

Executive Director

EMP Task Force on National and Homeland Security

Former Chief of Staff

Congressional EMP Commission

# Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

*Critical National Infrastructures*





# Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

## *Critical National Infrastructures*

### **Commission Members**

Dr. John S. Foster, Jr.

Mr. Earl Gjelde

Dr. William R. Graham (Chairman)

Dr. Robert J. Hermann

Mr. Henry (Hank) M. Kluepfel

Gen Richard L. Lawson, USAF (Ret.)

Dr. Gordon K. Soper

Dr. Lowell L. Wood, Jr.

Dr. Joan B. Woodard

**April 2008**





## Table of Contents

	<u>Page</u>
<b>Preface.....</b>	<b>vi</b>
<b>Acknowledgements .....</b>	<b>ix</b>
<b>Chapter 1. Infrastructure Commonalities.....</b>	<b>1</b>
SCADA Systems.....	1
Impact of SCADA Vulnerabilities on Critical Infrastructures: Historical Insight.....	6
Infrastructures and Their Interdependencies.....	9
Commission-Sponsored Modeling and Simulation (M&S) Activities .....	13
Summary .....	15
Recommendations.....	16
<b>Chapter 2. Electric Power .....</b>	<b>17</b>
Introduction.....	17
Description.....	20
Vulnerabilities.....	29
Test Results.....	37
Historical Insights .....	41
Distinctions .....	43
Strategy .....	45
Recommendations.....	53
<b>Chapter 3. Telecommunications.....</b>	<b>62</b>
Introduction.....	62
Telecommunications Support During Emergencies .....	64
EMP Impact on Telecommunications.....	65
Recommendations.....	79
<b>Chapter 4. Banking and Finance.....</b>	<b>83</b>
Introduction.....	83
The Financial Services Industry.....	85
Vulnerability to EMP .....	88
Consequences of Financial Infrastructure Failure .....	92
Recommendations.....	94
<b>Chapter 5. Petroleum and Natural Gas .....</b>	<b>95</b>
Introduction.....	95
Infrastructure Description .....	95
Direct Effects of EMP on Petroleum and Natural Gas Infrastructure.....	98
Petroleum Infrastructure and SCADA .....	98
Natural Gas Infrastructure and SCADA .....	99
Effects of an EMP Event on the U.S. Petroleum and Natural Gas Infrastructures.....	100
Indirect Effects of EMP: Accounting for Infrastructure Interdependencies .....	102
Recommendations.....	103
<b>Chapter 6. Transportation Infrastructure .....</b>	<b>105</b>
Introduction.....	105
Long-Haul Railroad .....	106
The Automobile and Trucking Infrastructures.....	112
Maritime Shipping .....	116

Commercial Aviation.....	122
Recommendations.....	127
<b>Chapter 7. Food Infrastructure.....</b>	<b>129</b>
Introduction.....	129
Dependence of Food on Other Infrastructures.....	129
Making, Processing, and Distributing Food.....	130
Vulnerability to EMP.....	132
Consequences of Food Infrastructure Failure.....	134
Recommendations.....	137
<b>Chapter 8. Water Infrastructure.....</b>	<b>139</b>
Introduction.....	139
The Water Works.....	140
Vulnerability to EMP.....	142
Consequences of Water Infrastructure Failure.....	143
Recommendations.....	146
<b>Chapter 9. Emergency Services.....</b>	<b>147</b>
Introduction.....	147
Emergency Services Systems Architecture and Operations.....	147
Impact of an EMP Attack.....	149
Recommendations.....	156
<b>Chapter 10. Space Systems.....</b>	<b>158</b>
Introduction.....	158
Terms of Reference for Satellites.....	159
Line-of-Sight Exposure to a Nuclear Detonation.....	159
Persistently Trapped Radiation and Its Effects.....	161
Nuclear Weapon Effects on Electronic Systems.....	162
Satellite Ground Stations.....	167
Discussion of Results.....	168
Findings.....	170
Recommendations.....	171
<b>Chapter 11. Government.....</b>	<b>172</b>
Introduction.....	172
Maintaining Government Connectivity and Coherence.....	172
Recommendations.....	172
<b>Chapter 12. Keeping The Citizenry Informed: Effects On People.....</b>	<b>176</b>
Introduction.....	176
Impact of an EMP Attack.....	176
Recommendations.....	181
<b>Appendix A. The Commission and Its Charter.....</b>	<b>A-1</b>
Organization.....	A-1
Method.....	A-2
Activities.....	A-2
<b>Appendix B. Biographies.....</b>	<b>B-1</b>

## List of Figures

	<u>Page</u>
Figure 1-1. Typical SCADA Architecture .....	2
Figure 1-2. Generic SCADA Architecture.....	3
Figure 1-3. PLC Switch Actuator .....	4
Figure 1-4. EMP Simulator with Test Structures and Internal Electronics .....	5
Figure 1-5. Some of the Electronic Control Systems Exposed in Test Facility .....	6
Figure 1-6. Physical Model Used to Quantify Coupling to Different Cable Lengths in a Hypothetical Local Area Network (LAN) .....	7
Figure 1-7. A Conceptual Illustration of the Interconnectedness of Elements Contained Within Each Critical Infrastructure. ....	12
Figure 1-8. Interdependency for Anticipated Network of the Future .....	14
Figure 1-9. Results of a Model Simulation .....	15
Figure 2-1. Power System Overview .....	21
Figure 2-2. NERC Interconnections .....	25
Figure 2-3. GIC Damage to Transformer During 1989 Geomagnetic Storm .....	33
Figure 2-4. EMP Simulator.....	38
Figure 2-5. Test Item: Electronic Relay.....	40
Figure 2-6. Flashover Observed During Injection Pulse Testing .....	41
Figure 3-1. Generic Telecommunications Network Architecture.....	66
Figure 3-2. September 11, 2001, Blocked Call Rate—Cellular Networks.....	70
Figure 3-3. Example Network Management Facility .....	71
Figure 3-4. Cellular Base Station Equipment .....	72
Figure 3-5. Routers Collecting Network Management Data .....	72
Figure 3-6. Cellular Network Testing at INL .....	74
Figure 3-7. Testing at NOTES Facility.....	74
Figure 3-8. Secure Access Card and Cell Phones.....	75
Figure 3-9. Percentage of Calls Completed Immediately After EMP Event.....	76
Figure 3-10. Percentage of Calls Completed 4 Hours After EMP Event .....	76
Figure 3-11. Percentage of Calls Completed 2 Days After EMP Event.....	77
Figure 3-12. Percentage of Calls Completed at Time T (Logarithmic Time Scale) (Within EMP Contours).....	77
Figure 5-1. Petroleum Infrastructure.....	96
Figure 5-2. Natural Gas Infrastructure.....	97
Figure 5-3. Typical SCADA Arrangement for Oil Operations.....	99
Figure 5-4. SCADA Integrates Control of Remote Natural Gas Facilities.....	100
Figure 5-5. Examples of Oil Interdependencies .....	102
Figure 5-6. Examples of Natural Gas Interdependencies .....	102
Figure 6-1. 2003 Class I Railroad Tons Originated.....	107
Figure 6-2. CSXT Train Dispatch Center .....	108
Figure 6-3. Typical Block Signal Control Equipment Enclosure .....	110
Figure 6-4. Grade Crossing Shelter and Sensor Connection .....	110
Figure 6-5. Modern Locomotive Functional Block Diagram .....	111
Figure 6-6. A Typical Signalized Intersection.....	113
Figure 6-7. Container Cranes and Stored Containers .....	117
Figure 6-8. RTG at Seagirt Marine Terminal .....	118
Figure 6-9. Handheld Wireless Data Unit.....	119

Figure 6-10. Truck Control Station.....	119
Figure 6-11. An ARTCC Operations Room .....	122
Figure 9-1. A Generic Modern Emergency Services System .....	148
Figure 10-1. From left to right, the ORANGE, TEAK, KINGFISH, CHECKMATE, and STARFISH high-altitude nuclear tests conducted in 1958 and 1962 by the United States near Johnston Island in the mid- Pacific .....	159
Figure 10-2. Satellite Orbits Illustrated .....	159
Figure 10-3. Areas of Space Irradiated by Photons and Neutrons.....	160
Figure 10-4. Naturally occurring belts (Van Allen belts) of energetic particles persistently trapped in the geomagnetic field are illustrated .....	161
Figure 10-5. Schematic diagram of relative intensities of trapped fluxes from two identical high-altitude nuclear detonations .....	161
Figure 10-6. Satellites remaining after a 10 MT burst over Lake Superior .....	167
Figure 10-7. Satellite ground-based receiver outage time after a 10 MT burst over Lake Superior.....	167
Figure 10-8. HEO satellite exposure to trapped radiation produced by Events 11, 17, and 21 .....	168

### List of Tables

Table 3-1. Telecommunications Equipment Tested .....	73
Table 10-1. Trial Nuclear Events.....	163
Table 10-2. Analysis of Satellites .....	164
Table 10-3. Probability That Satellites Suffer Damage by Direct Exposure to X-Rays .....	165
Table 10-4. Trial Events in Group 1 .....	165
Table 10-5. Trial Events in Group 2 .....	166
Table 10-6. Trial Events in Group 3 .....	166

## Preface

The physical and social fabric of the United States is sustained by a system of systems; a complex and dynamic network of interlocking and interdependent infrastructures (“critical national infrastructures”) whose harmonious functioning enables the myriad actions, transactions, and information flow that undergird the orderly conduct of civil society in this country. The vulnerability of these infrastructures to threats — deliberate, accidental, and acts of nature — is the focus of greatly heightened concern in the current era, a process accelerated by the events of 9/11 and recent hurricanes, including Katrina and Rita.

This report presents the results of the Commission’s assessment of the effects of a high altitude electromagnetic pulse (EMP) attack on our critical national infrastructures and provides recommendations for their mitigation. The assessment is informed by analytic and test activities executed under Commission sponsorship, which are discussed in this volume. An earlier executive report, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) — Volume 1: Executive Report* (2004), provided an overview of the subject.

The electromagnetic pulse generated by a high altitude nuclear explosion is one of a small number of threats that can hold our society at risk of catastrophic consequences. The increasingly pervasive use of electronics of all forms represents the greatest source of vulnerability to attack by EMP. Electronics are used to control, communicate, compute, store, manage, and implement nearly every aspect of United States (U.S.) civilian systems. When a nuclear explosion occurs at high altitude, the EMP signal it produces will cover the wide geographic region within the line of sight of the detonation.<sup>1</sup> This broad band, high amplitude EMP, when coupled into sensitive electronics, has the capability to produce widespread and long lasting disruption and damage to the critical infrastructures that underpin the fabric of U.S. society.

Because of the ubiquitous dependence of U.S. society on the electrical power system, its vulnerability to an EMP attack, coupled with the EMP’s particular damage mechanisms, creates the possibility of long-term, catastrophic consequences. The implicit invitation to take advantage of this vulnerability, when coupled with increasing proliferation of nuclear weapons and their delivery systems, is a serious concern. A single EMP attack may seriously degrade or shut down a large part of the electric power grid in the geographic area of EMP exposure effectively instantaneously. There is also a possibility of functional collapse of grids beyond the exposed area, as electrical effects propagate from one region to another.

The time required for full recovery of service would depend on both the disruption and damage to the electrical power infrastructure and to other national infrastructures. Larger affected areas and stronger EMP field strengths will prolong the time to recover. Some critical electrical power infrastructure components are no longer manufactured in the United States, and their acquisition ordinarily requires up to a year of lead time in routine circumstances. Damage to or loss of these components could leave significant parts of the electrical infrastructure out of service for periods measured in months to a year or more. There is a point in time at which the shortage or exhaustion of sustaining backup systems,

---

<sup>1</sup> For example, a nuclear explosion at an altitude of 100 kilometers would expose 4 million square kilometers, about 1.5 million square miles, of Earth surface beneath the burst to a range of EMP field intensities.

including emergency power supplies, batteries, standby fuel supplies, communications, and manpower resources that can be mobilized, coordinated, and dispatched, together lead to a continuing degradation of critical infrastructures for a prolonged period of time.

Electrical power is necessary to support other critical infrastructures, including supply and distribution of water, food, fuel, communications, transport, financial transactions, emergency services, government services, and all other infrastructures supporting the national economy and welfare. Should significant parts of the electrical power infrastructure be lost for any substantial period of time, the Commission believes that the consequences are likely to be catastrophic, and many people may ultimately die for lack of the basic elements necessary to sustain life in dense urban and suburban communities. In fact, the Commission is deeply concerned that such impacts are likely in the event of an EMP attack unless practical steps are taken to provide protection for critical elements of the electric system and for rapid restoration of electric power, particularly to essential services. The recovery plans for the individual infrastructures currently in place essentially assume, at worst, limited upsets to the other infrastructures that are important to their operation. Such plans may be of little or no value in the wake of an EMP attack because of its long-duration effects on all infrastructures that rely on electricity or electronics.

The ability to recover from this situation is an area of great concern. The use of automated control systems has allowed many companies and agencies to operate effectively with small work forces. Thus, while manual control of some systems may be possible, the number of people knowledgeable enough to support manual operations is limited. Repair of physical damage is also constrained by a small work force. Many maintenance crews are sized to perform routine and preventive maintenance of high-reliability equipment. When repair or replacement is required that exceeds routine levels, arrangements are typically in place to augment crews from outside the affected area. However, due to the simultaneous, far-reaching effects from EMP, the anticipated augmenters likely will be occupied in their own areas. Thus, repairs normally requiring weeks of effort may require a much longer time than planned.

The consequences of an EMP event should be prepared for and protected against to the extent it is reasonably possible. Cold War-style deterrence through mutual assured destruction is not likely to be an effective threat against potential protagonists that are either failing states or trans-national groups. Therefore, making preparations to manage the effects of an EMP attack, including understanding what has happened, maintaining situational awareness, having plans in place to recover, challenging and exercising those plans, and reducing vulnerabilities, is critical to reducing the consequences, and thus probability, of attack. The appropriate national-level approach should balance prevention, protection, and recovery.

The Commission requested and received information from a number of Federal agencies and National Laboratories. We received information from the North American Electric Reliability Corporation, the President's National Security Telecommunications Advisory Committee, the National Communications System (since absorbed by the Department of Homeland Security), the Federal Reserve Board, and the Department of Homeland Security. Early in this review it became apparent that only limited EMP vulnerability testing had been accomplished for modern electronic systems and components. To partially remedy this deficit, the Commission sponsored illustrative



testing of current systems and infrastructure components. The Commission's view is that the Federal Government does not today have sufficiently robust capabilities for reliably assessing and managing EMP threats.

The United States faces a long-term challenge to maintain technical competence for understanding and managing the effects of nuclear weapons, including EMP. The Department of Energy and the National Nuclear Security Administration have developed and implemented an extensive Nuclear Weapons Stockpile Stewardship Program over the last decade. However, no comparable effort was initiated to understand the effects that nuclear weapons produce on modern systems. The Commission reviewed current national capabilities to understand and to manage the effects of EMP and concluded that the Country is rapidly losing the technical competence in this area that it needs in the Government, National Laboratories, and Industrial Community.

An EMP attack on the national civilian infrastructures is a serious problem, but one that can be managed by coordinated and focused efforts between industry and government. It is the view of the Commission that managing the adverse impacts of EMP is feasible in terms of time and resources. A serious national commitment to address the threat of an EMP attack can develop a national posture that would significantly reduce the payoff for such an attack and allow the United States to recover in a timely manner if such an attack were to occur.



## Acknowledgements

The Commission is pleased to acknowledge the support of its staff, whose professionalism and technical competence have contributed substantially to this report:

- ◆ Dr. George Baker
- ◆ Dr. Yvonne Bartoli
- ◆ Mr. Fred Celec
- ◆ Dr. Edward Conrad
- ◆ Dr. Michael Frankel
- ◆ Dr. Ira Kohlberg
- ◆ Dr. Rob Mahoney
- ◆ Dr. Mitch Nikolich
- ◆ Dr. Peter Vincent Pry
- ◆ Dr. James Scouras
- ◆ Dr. James Silk
- ◆ Ms. Shelley Smith
- ◆ Dr. Edward Toton

The Commission additionally acknowledges the technical and scientific contributions of Dr. William Radasky, Dr. Jerry Lubell, Mr. Walter Scott, Mr. Paul F. Spraggs, Dr. Al Costantine, Dr. Gerry Gurtman, Dr. Vic Van Lint, Dr. John Kappenman, Dr. Phil Morrison, Mr. John Bombardt, Mr. Bron Cikotas, Mr. David Ambrose, Dr. Bill White, Dr. Yacov Haimen, Dr. Rebecca Edinger, Ms. Rachel Balsam and Mr. Chris Baker. The Commission also acknowledges the cooperation and assistance of Ms. Linda Berg; Dr. Dale Klein (former Assistant to the Secretary of Defense [Nuclear, Chemical, and Biological Matters]); the leadership of the Defense Threat Reduction Agency and its Commission liaison, Ms. Joan Pierre; Dr. Don Linger, Senior Scientist at the Defense Threat Reduction Agency; Dr. David Stoudt of the Naval Surface Warfare Center-Dahlgren; Dr. Michael Bernardin of Los Alamos National Laboratory; and Dr. Tom Thompson and Dr. Todd Hoover of the Lawrence Livermore National Laboratory.

We also acknowledge the cooperation of the Intelligence Community (IC).

The Commission was ably supported by the contracted research activities of the following organizations: the National Nuclear Security Administration's laboratories (Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Sandia National Laboratory), Argonne National Laboratory, Idaho National Laboratory, Naval Surface Warfare Center-Dahlgren, the Institute for Defense Analyses, Jaycor/Titan, Metatech Corporation, Science Applications International Corporation, Telcordia Technologies, Mission Research Corporation, and the University of Virginia Center for Risk Management of Engineering Systems.



## Chapter 1. Infrastructure Commonalities

The physical and social fabric of the United States is sustained by a system of systems; a complex and dynamic network of interlocking and interdependent infrastructures (“critical national infrastructures”) whose harmonious functioning enables the myriad actions, transactions, and information flow that undergird the orderly conduct of civil society in this country. The vulnerability of these infrastructures to threats — deliberate, accidental, and acts of nature — is the focus of heightened concern in the current era, a process accelerated by the events of 9/11 and recent hurricanes, including Katrina and Rita.

This volume focuses on a description of the potential vulnerabilities of our critical national infrastructures to electromagnetic pulse (EMP) insult, and to that end, the chapters in this document deal individually with the EMP threat to each critical infrastructure separately. However, to set the stage for understanding the potential threat under conditions in which all infrastructures are under simultaneous attack, it is important to realize that the vulnerability of the whole — of all the highly interlocked critical infrastructures — may be greater than the sum of the vulnerability of its parts. The whole is a highly complex system of systems whose exceedingly dynamic and coordinated activity is enabled by the growth of technology and where failure within one individual infrastructure may not remain isolated but, instead, induce cascading failures into other infrastructures.

It is also important to understand that not only mutual interdependence, and hence new vulnerabilities, may be enabled by technology advances, but also technologies that have facilitated this growing interdependence may be common across the many individual infrastructures. In particular, the Commission thought it important to single out the growth and common infrastructural infiltration of one particular transformative technology, the development of automated monitoring and control systems — the ubiquitous robots of the modern age known as Supervisory Control and Data Acquisition (SCADA) systems.

This opening chapter thus focuses on a more detailed description of these two aspects of modern infrastructures, control systems and mutual interdependence, that are common to all and which the Commission believes provide context and insight for understanding sources of vulnerability in all the Nation’s infrastructures to EMP attack.

### SCADA Systems

#### *Introduction*

SCADAs have emerged as critical and growing elements of a quietly unfolding industrial revolution spurred by the computer age. The accelerating penetration of SCADA systems, along with their electronic cousins, digital control systems (DCS) and programmable logic controllers (PLC), as critical elements in every aspect of every critical infrastructure in the Nation, is both inevitable and inexorable. While conferring economic benefit and enormous new operational agility, the growing dependence of our infrastructures on these omnipresent control systems represents a new vector of vulnerability in the evolving digital age of the 21st century, such as cyber security. Such issues remain as a matter for high-level concern and attention today. High-altitude EMP focuses our attention toward another potential vulnerability of these systems, and one with potentially vastly expanded consequences.

### What Is a SCADA?

SCADAs are electronic control systems that may be used for data acquisition and control over large and geographically distributed infrastructure systems. They find extensive use in critical infrastructure applications such as electrical transmission and distribution, water management, and oil and gas pipelines. SCADA technology has benefited from several decades of development. It has its genesis in the telemetry systems used by the railroad and aviation industries.

*In November 1999, San Diego County Water Authority and San Diego Gas and Electric companies experienced severe electromagnetic interference to their SCADA wireless networks. Both companies found themselves unable to actuate critical valve openings and closings under remote control of the SCADA electronic systems. This inability necessitated sending technicians to remote locations to manually open and close water and gas valves, averting, in the words of a subsequent letter of complaint by the San Diego County Water Authority to the Federal Communications Commission, a potential "catastrophic failure" of the aqueduct system. The potential consequences of a failure of this 825 million gallon per day flow rate system ranged from "spilling vents at thousands of gallons per minute to aqueduct rupture with ensuing disruption of service, severe flooding, and related damage to private and public property." The source of the SCADA failure was later determined to be radar operated on a ship 25 miles off the coast of San Diego.*

The physical form of a SCADA may differ from application to application and from one industry to another, but generally they all share certain generic commonalities. A SCADA system physically bears close resemblance to the internals of a generic desktop personal computer. Typically, it might contain familiar-appearing circuit boards, chips of various sorts, and cable connectors to the external world. The cable connectors, in turn, may be connected, perhaps quite remotely, to various sensor systems that are the SCADA's eyes and ears, as well as electronic control devices by which the SCADA may issue commands that adjust system performance. **Figure 1-1** provides an example of a particular SCADA controller that is representative of many such systems.

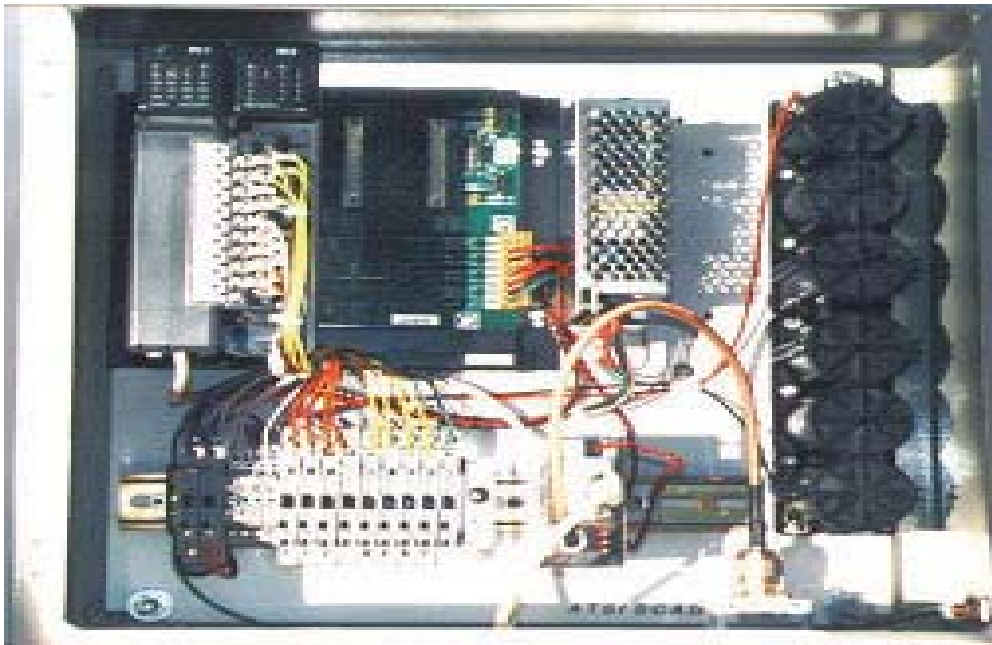


Figure 1-1. Typical SCADA Architecture

One major function of a SCADA — the data acquisition part of the acronym — is to provide a capability to automatically and remotely monitor the operating state of a physical system. It accomplishes this monitoring by providing an ongoing reporting of parameters that either characterize the system's performance, such as voltage or currents developed in an electric power plant, flow volume in a gas pipeline, and net electrical power delivered or received by a regional electrical system, or by monitoring environmental parameters such as temperature in a nuclear power plant and sending an alarm when prescribed operating conditions are exceeded.

The supervisory control function of a SCADA reflects the ability of these devices to actively control the operation of the system by adjusting its output. For example, should an electrical generating plant fail through loss of a critical hardware component or industrial accident, the monitoring SCADA will detect the loss, issue an alert to the appropriate authorities, and issue commands to other generating plants under its control to increase their power output to match the load again. All these actions take place automatically, within seconds, and without a human being involved in the immediate control loop.

A typical SCADA architecture for the electric power industry may consist of a centralized computer — the master terminal unit (MTU) — communicating through many remote terminal unit (RTU) subsystems, as illustrated in **figure 1-2**. The RTUs are used in remote, unmanned locations where data acquisition and control tasks must be performed. Examples of typical RTU data acquisition actions include processing signals from sensors such as thermocouples, voltage sensors, or power meters and reporting the state of equipment such as switch and circuit breaker positions. Typical control actions include starting and stopping motors and controlling valves and circuit breakers.

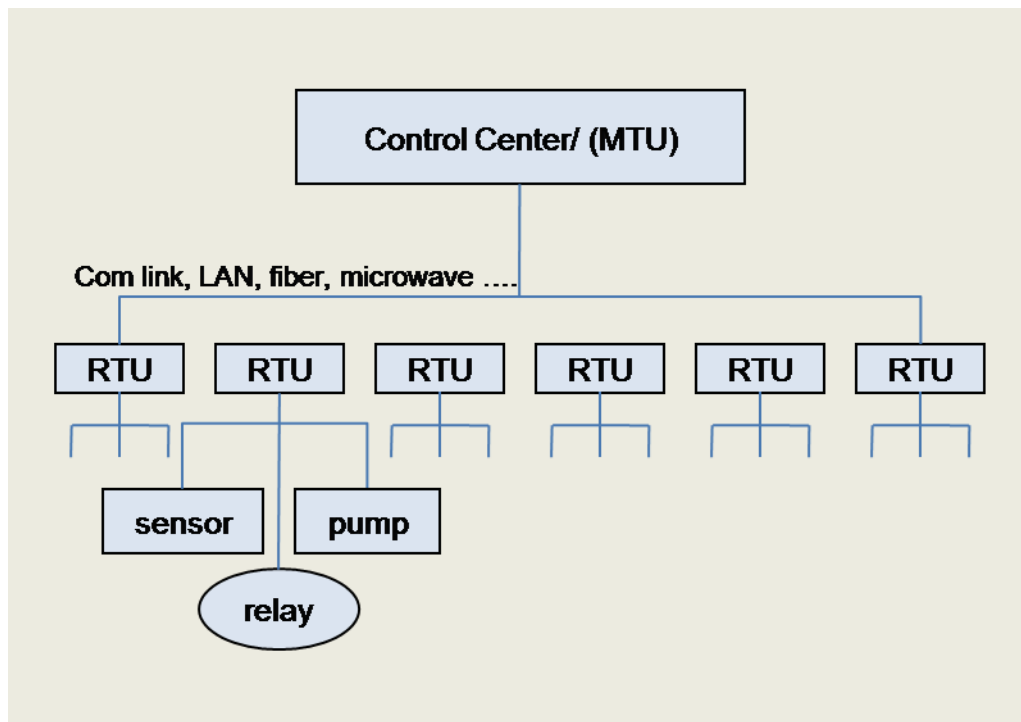


Figure 1-2. Generic SCADA Architecture

DCSs share many functional and physical hardware similarities with SCADA systems. A DCS typically will be used to control automated processes at a single location, such as



an oil refinery or a chemical plant. In contrast, a SCADA typically might be sited in an environment with dispersed assets where real-time situational awareness from remote locations is a key element of centralized control. Most DCS installations control complex, dynamic systems that would be difficult or impossible to control in a safe or economical manner using only manual control.

Even a relatively straightforward process such as electrical power generation using a conventional steam cycle requires highly complex systems to maximize efficiency, while maintaining safety and environmental protection. For example, control systems in a steam generating plant would include parameters such as generator speed, generator lubrication oil pressure, excitation current and voltage output, feed water pressure and boiler steam drum level, and air box pressure and rate of combustion.

Upset of these control points has the potential to cause severe physical damage. A case in point is the boiler endpoints of combustion and circulation. Normally, the control system would first reach the endpoint of combustion (limit of air and fuel adding energy into the boiler) and, thus, prevent any thermal damage to the boiler. If the control system is upset, it potentially could reach the endpoint of circulation (maximum rate of steam generation) or endpoint of carryover (maximum rate at which water is *not* carried out of the boiler) before the endpoint of combustion. This situation would cause thermal damage to the boiler tubes or physical damage to steam turbine blades.

Normally, a PLC is used to control actuators or monitor sensors and is another piece of hardware that shares many physical similarities to SCADAs and is often found as part of a larger SCADA or DCS system. The SCADA, DCS, and PLC systems all share electronic commonalities and, thus they share intrinsic electronic vulnerabilities as well. SCADA systems, however, tend to be more geographically disposed and exposed; our subsequent discussion focuses on SCADAs. When exposure or unprotected cable connectivity is an issue, the discussion should be considered to pertain to both PLC and DCS as well. See **figure 1-3**.

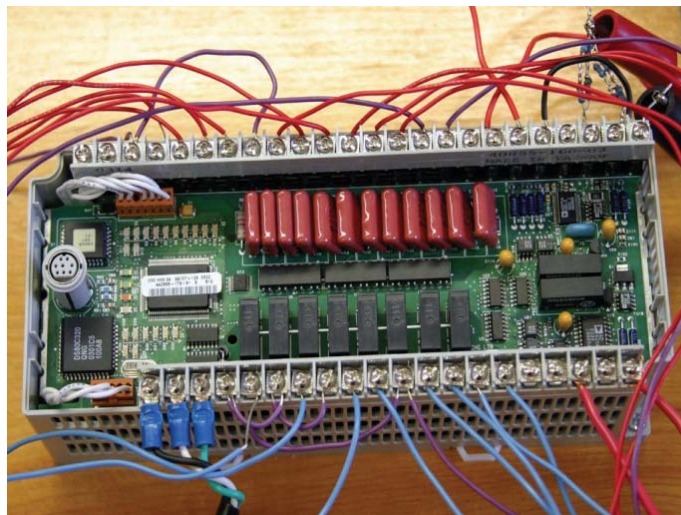


Figure 1-3. PLC Switch Actuator

### ***EMP Interaction with SCADA***

SCADA system components by their nature are frequently situated in remote environments and operate without proximate human intervention. Although their critical electronic elements usually are contained within some sort of metallic box, the enclosures'

service as a protective Faraday cage is typically minimal. Generally such metallic containers are designed only to provide protection from the elements and a modicum of physical security. They typically are not designed to protect the electronics from high-energy electromagnetic pulses that may infiltrate either from the free field or from the many antennae (cable connections) that may compromise electromagnetic integrity. The major concern for SCADA vulnerability to EMP is focused on the early time E1 component of the EMP signal. This is because, even in the power industry, SCADA systems generally are not directly coupled electrically to the very long cable runs that might be expected to couple to a late-time E3 signal.

To come to grips with the potential vulnerability of our critical national infrastructures caused by a threat to these ubiquitous SCADA control systems, we must first develop a sense of the vulnerability of the underlying hardware components themselves. To this end, the EMP Commission sponsored and funded a series of tests of common SCADA components in a government-owned EMP simulator (see **figure 1-4**). The simulation testing provided an opportunity to observe the interaction of the electromagnetic energy with equipment in an operational mode. Because the simulator did not completely replicate all characteristics of a threat-level EMP environment, observed test results can be related to the system's response in more realistic scenarios through analysis and judgment based on coupling differences between the simulated and real-world cases.



**Figure 1-4. EMP Simulator with Test Structures and Internal Electronics**

The Commission consulted with experts from industry groups associated with the North American Electric Reliability Corporation (NERC) and by site and market surveys to identify representative control systems for testing. A test matrix was developed that reflected electronic control technologies employed in power generation, power distribution, pipeline distribution, and manufacturing plants. Some test items assessed in this effort are shown in **figure 1-5**.



Figure 1-5. Some of the Electronic Control Systems Exposed in Test Facility

### ***EMP Simulation Testing***

In this section, we provide a brief summary of the results of illuminating electronic control systems in the simulator. The detailed results of the simulation test program are documented separately in reports sponsored by the Commission. In Chapter 2, we provide a more complete description of the test methodology, in which we discuss testing carried out during assessment of the EMP vulnerability of the electric grid.

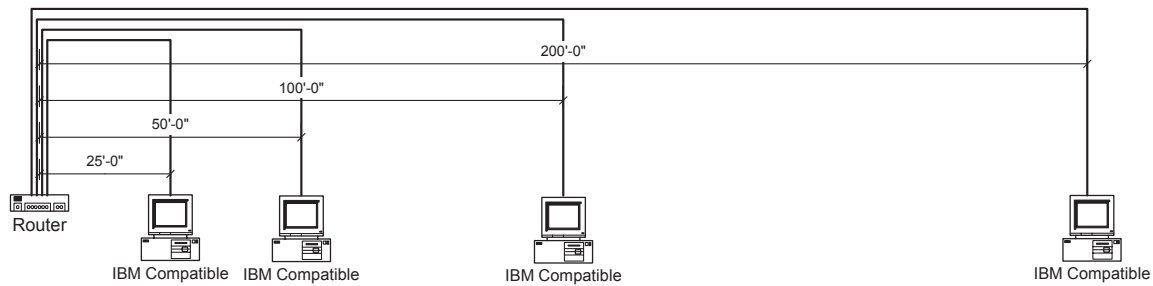
Many of the control systems that we considered achieved operational connectivity through Ethernet cabling. EMP coupling of electrical transients to the cables proved to be an important vulnerability during threat illumination. Because the systems would require manual repair, their full restoration could be a lengthy process. A simple model of four Ethernet cables from a router to four personal computers (PC) was generated to quantify the impact of cable length. The configuration of this model is shown in **figure 1-6**. The results of the analysis indicate that the coupling to the 200 feet of Ethernet line is roughly seven times the transient level on the 25-foot line measured during the test program. The testing and analysis indicate that the electronics could be expected to see roughly 100 to 700 ampere current transients on typical Ethernet cables. Effects noted in the EMP testing occurred at the lower end of this scale.

The bottom line observation at the end of the testing was that every system tested failed when exposed to the simulated EMP environment. The failures were not identical from system to system or within a system. For example, a device with many input-output ports might exhibit degraded performance on one port, physical damage on another, and no effect on a third. Control units might report operating parameters at variance with their post illumination reality or fail to control internal flows. The Commission considered the implications of these multiple simultaneous control system failures to be highly significant as potential contributors to a widespread system collapse.

### **Impact of SCADA Vulnerabilities on Critical Infrastructures: Historical Insight**

Based on the testing and analysis outlined in the previous section, we estimate that a significant fraction of all remote control systems within the EMP-affected area will





**Figure 1-6. Physical Model Used to Quantify Coupling to Different Cable Lengths in a Hypothetical Local Area Network (LAN)**

experience some type of impact. As the test results were briefed to industry experts at NERC and the Argonne National Laboratory, it became apparent that even minor effects noted during the testing could significantly affect the processes and equipment being controlled. Putting together a complete analysis for complex processes associated with infrastructure systems is extremely difficult. Developing the ability to analyze or model these impacts is beyond the scope of this effort.

To provide insight into the potential impact of these EMP-induced electronic system malfunctions, one can consider the details of historical events. In these cases, similar (and arguably less severe) system malfunctions have produced consequences in situations that are far too complex to predict beforehand using a model or analysis.

Another important observation is that these incidents are seldom the result of a single factor. Rather they are a combination of unexpected events that, only in hindsight, are easily related to the impact. This is not surprising given the complexity of the systems involved. Before considering the historical database, it is important to remember that historical examples, although important for the insight they provide into the dependence of a functioning modern infrastructure on its automated eyes, ears, and remote controllers, do not adequately capture the scale of the expected EMP scenario. In the latter, it is not one or a few SCADA systems that are malfunctioning (the typical historical scenario), but large numbers — hundreds or even thousands — with some fraction of those rendered permanently inoperable until replaced or physically repaired.

Significant historical events that provide insight into the potential impact of damage or upset to control systems include Hurricane Katrina; the 1996 Western States blackout; the August 14, 2003, Northeast blackout; a geomagnetic storm in 1989; the June 10, 1999, Bellingham pipeline incident; the August 19, 2000, Carlsbad pipeline incident; the July 24, 1994, Pembroke, United Kingdom, refinery incident; and a Netherlands electromagnetic interference (EMI) incident. The following paragraphs discuss the relevance of four of these incidents to an EMP event. The other four incidents — Hurricane Katrina; the Western States blackout; the August 14, 2003, blackout; and the 1989 geomagnetic storm — are described in Chapter 2, which is dedicated to a discussion of EMP effects on the electric power grid.

*Bellingham Pipeline Incident.* On June 10, 1999, one of the Olympic pipelines transporting gasoline ruptured in the Whatcom Falls Park area of Bellingham, Washington. About 250,000 gallons of gasoline from the pipeline entered the Hannah and Whatcom Creeks, where the fuel ignited, resulting in three fatalities and eight injuries. In addition, the banks of the creek were destroyed over a 1.5-mile section, and several buildings adjacent to the creek were severely damaged.

Causes included improperly set relief valves, delayed maintenance inspections, and SCADA system discrepancies. The effects all came together at the same time that changes in pipeline operations were occurring. Given the wide area of an EMP, it is conceivable that some of the pipelines affected could also suffer from poor maintenance. The electronic disturbance of an EMP event could be expected to precipitate SCADA failures and the ensuing loss of valve controls.

*Carlsbad Pipeline Incident.* On August 19, 2000, an explosion occurred on one of three adjacent large natural gas pipelines near Carlsbad, New Mexico, operated by the El Paso Natural Gas Company. The pipelines supply consumers and electric utilities in Arizona and Southern California. Twelve people, including five children, died as a result of the explosion. The explosion left an 86-foot-long crater. After the pipeline failure, the Department of Transportation's Office of Pipeline Safety (OPS) ordered the pipeline to be shut down. The explosion happened because of failures in maintenance and loss of situational awareness, conditions that would be replicated by data acquisition disruptions caused by an EMP event.

*Pembroke Refinery Incident.* On July 24, 1994, a severe thunderstorm passed over the Pembroke refinery in the United Kingdom. Lightning strikes resulted in a 0.4 second power loss and subsequent power dips throughout the refinery. Consequently, numerous pumps and overhead fin-fan coolers tripped repeatedly, resulting in the main crude column pressure safety valves lifting and major upsets in the process units in other refinery units, including those within the fluid catalytic cracking (FCC) complex.

There was an explosion in the FCC unit and a number of isolated fires continued to burn at locations within the FCC, butamer, and alkylation units. The explosion was caused by flammable hydrocarbon liquid continuously being pumped into a process vessel that, because of a valve malfunction, had its outlet closed. The control valve was actually shut when the control system indicated that it was open. The malfunctioning process control system did not allow the refinery operators to contain the situation.

As a result of this incident, an estimated 10 percent of the total refining capacity in the United Kingdom was lost until this complex was returned to service. The business loss is estimated at \$70 million, which reflects 4.5 months of downtime. The disturbances caused by the lightning strikes — power loss and degradation — would also result from an EMP event.

*Netherlands EMI Incident.* A mishap occurred at a natural gas pipeline SCADA system located about 1 mile from the port of Den Helder, Netherlands, in the late 1980s. A SCADA disturbance caused a catastrophic failure of an approximately 36-inch diameter pipeline, which resulted in a large gas explosion.

This failure was caused by EMI traced to a radar coupling into the wires of the SCADA system. Radio frequency energy caused the SCADA system to open and close at the radar scan frequency, a relay that was, in turn, controlling the position of a large gas flow-control valve. The resulting changes in valve position created pressure waves that traveled down the pipeline and eventually caused the pipeline to fail. This incident shows the potential damage to pipelines from improper control system operations, a condition that could be replicated by an EMP event.

## Summary

SCADA systems are vulnerable to EMP insult. The large numbers and widespread reliance on such systems by all of the Nation's critical infrastructures represent a systemic threat to their continued operation following an EMP event. Additionally, the necessity to reboot, repair, or replace large numbers of geographically widely dispersed systems will considerably impede the Nation's recovery from such an assault.

## Infrastructures and Their Interdependencies

### Introduction

All critical national infrastructures are fault tolerant to some degree. Design engineers and system managers are cognizant of, and fully expect, failure of subsystems and individual electrical components. Networks are designed with an expressed goal to avoid single point failures that can bring down the entire system, though in practice the evolved network may be so complicated that no one can guarantee that this design goal has been achieved. Single point failures are anticipated in the design of the systems and engineering solutions of various kinds, including redundancy, rapid repair, replacement, and operational rerouting.

It is important to note, however, that safeguards against single point failures generally depend on the proper functioning of the rest of the national infrastructure, a plausible assumption for high-reliability infrastructure systems when they experience random, uncorrelated single point failures.

Planning for multiple failures, particularly when they are closely correlated in time, is much less common. It is safe to say that no one has planned for, and few have even imagined, a scenario with the loss of hundreds or even thousands of nodes across all the critical national infrastructures, all simultaneously. That, however, is precisely the circumstance contemplated by an EMP attack scenario.

The ability to predict the consequences of failure within a critical infrastructure will require the use of reliable modeling and simulation tools. Some tools exist for the individual infrastructures and serve as either planning tools, real-time control models, or operational support elements to allocate or control resources during network outages and restoration activities.

They are generally validated within the parameter space of normal operating experience and concern, and they serve their purposes well. But it is also recognized that the systems being modeled are so complex that currently available modeling tools cannot capture the full richness of potential system responses to all possible network configurations and operating states.

Thus, for example, on the order of once a decade or so, portions of the national power grid will experience an unpredicted major disruption with failures cascading through some of the network pathways. Following the major Northeast power blackout of August 14, 2003, analysts continued to debate the cause of the disruption. The sophisticated, relatively mature, and operationally deployed modeling and simulation tools have not been able to replicate unambiguously the observed events of August 14.

◆  
“We have produced designs so complicated that we cannot possibly anticipate all the possible interactions of the inevitable failures; we add safety devices that are deceived or avoided or defeated by hidden paths in the systems.” Charles Perrow, *Normal Accidents*

The scenarios envisioned by an EMP attack involve potential failures distributed across a wide geographical extent. These include multiple combinations of node failures, a condition that generally is outside the parameter space of validation of extant system models and poses a severe challenge to predicting the subsequent evolution of the infrastructure response. The response of critical national infrastructures to an EMP attack is precisely the subject of many sections of this report. But there is a particular aspect of modeling infrastructures that is even less well developed and whose particular relevance to the EMP scenario stresses the current state of the simulation art to produce a high-fidelity simulation. That aspect is the interaction among the different infrastructures. Particularly difficult to anticipate and to capture in simulations are situations in which the occurrence of simultaneous failures can bring into play dormant and hitherto hidden interaction pathways in which a destructively synergistic amplification of failure, normally locally contained, may be propagated through the network at large.

Charles Perrow<sup>1</sup> in particular has drawn attention to these types of failures, which he has termed *normal accidents* and which are posited as an inherent property of any tightly coupled system once a threshold of complexity has been passed. The Commission believes that, given sufficient priority, time and resources, complex interdependent models can be developed to guide future assessments of the U.S. national infrastructure to EMP attack and to guide investment decisions on how best to protect our infrastructures.

### **Complex Interactions**

Various lists are in circulation that identify the critical infrastructures. The EMP Commission has chosen to address the following areas in separate sections of this Commission report:

- ◆ Electric power
- ◆ Telecommunications
- ◆ Banking and finance
- ◆ Petroleum and natural gas
- ◆ Transportation
- ◆ Food
- ◆ Water
- ◆ Emergency services
- ◆ Space
- ◆ Government

The separation of these infrastructures into different domains tends to obscure the real interdependencies that sustain the effectiveness and daily operation of each one.

As a simple example, the telecommunications infrastructure requires power that is delivered by the power infrastructure. If power delivery is disrupted by disturbances in the power grid, telecommunication substations will run for a while on reserve battery power but would then need to switch to reserve backup generators (if they have them). The generator's operation would rely on fuel, first from on-site storage and then conveyed to a central distribution point by the energy distribution infrastructure and delivered to the telecommunications substation by the transportation infrastructure and paid for by the components of the financial infrastructure. The technicians who show up,

---

<sup>1</sup> Perrow, Charles, *Normal Accidents*, Princeton University Press, Princeton, N.J., 1999.



through the transportation infrastructure, to make repairs would not do so unless they have been sustained by the food and water delivery infrastructures, and so forth. In turn, a functioning telecommunications system provides critical situational awareness and control to a power infrastructure that must keep its power generation in balance with its load in a dynamic control process over a very large geographical area. Telecommunications also plays a critical role in controlling the transportation system and is the basis of data exchange within the financial infrastructure. The complex interdependence between elements within each infrastructure is suggested and illustrated schematically but by no means wholly characterized by **figure 1-7**.

◆  
“Communicating across disciplines requires domain experts to learn one another’s language to pose significant questions and usefully interpret answers,” National Academy of Sciences, *Making the Nation Safer; The Role of Science and Technology in Countering Terrorism*

In the course of ordinary interruptions, many of these infrastructure interdependencies and interactions can be safely ignored. In an EMP attack scenario, the immediate insult is expected to affect the different infrastructures simultaneously through multiple electronic component disruptions and failures over a wide geographical area. Understanding these cross-cutting interdependencies and interactions is critical to assessing the capability of the full system of interdependent critical infrastructures to recover. The modeling and simulation needed to explore the response of such a complex situation involves a large but finite number of elements and should be amenable to analysis, at least approximately, but little effort has been made to address the problem to date.

In practice, understanding the interdependence may be a difficult task because subject area experts are not necessarily attuned to coupling mechanisms that span the boundary between their respective discipline and another, and because an accurate representation of the interdependence requires a familiarity with transdisciplinary phenomena.

Experience demonstrates that it is sometimes easy to overlook the less obvious roles that such interdependencies and interactions may play, and coupling pathways may be easily overlooked. As an example, many of the recovery procedures developed by organizations to deal with emergencies involve the implicit assumption that transportation is available and people will be put on airplanes and go somewhere to diagnose and repair something. In the immediate aftermath of 9/11, all civilian airplanes were grounded. In 1991, a single point failure inside the telecommunications system, the accidental severing of a single fiber-optic cable in the New York City region, not only blocked 60 percent of all calls into and out of New York, but also disabled all air traffic control functions from Washington, D.C., to Boston — the busiest flight corridor in the Nation — and crippled the operations of the New York Mercantile Exchange.<sup>2</sup> These key interdependencies were always there, but they were not recognized as warranting advanced contingency planning, situational awareness in degraded conditions, and operational workarounds.

---

<sup>2</sup> Neumann, Peter, *Computer-Related Risks*, Addison Wesley, Reading, Mass., 1995.



Infrastructure vulnerability has been the subject of recent high-level attention with three separate congressionally chartered commissions devoted to the topic, including the President's Commission on Critical Infrastructures (the Marsh Commission), the EMP Commission and The National Research Council of the National Academy of Sciences. The latter issued a report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* in 2002, which explores potential vulnerabilities in the same list of critical infrastructures cited in the previous section. Both commissions noted the lack of a mature modeling and simulation capability as a significant weakness in the protective toolset available to planners and those charged with the mission of shielding our key infrastructures from subversion or other disruption. The National Academy of Sciences study, in particular, recommended the development of an analytic capability based on systems engineering principles.

Critical infrastructure studies also have been a growing activity in academia with the participation of individual scholars at various universities around the country. A number of academic centers have also set up or spun off entire institutes devoted to the analysis of critical infrastructural matters. The University of Virginia has created the Center for Risk Management, which focuses on the application of input-output econometric models

to analysis of critical infrastructures. In addition, George Mason and James Madison universities in Virginia have created the Center for Infrastructure Protection Programs (CIPP). The Santa Fe Institute of Complexity Studies also has pursued important theoretical work, and there are many other examples as well.

These efforts, as well as other important related work, are pointing in the right direction. Nevertheless, the bottom-line is that currently an adequate capability to model individual infrastructures on a national scale does not exist. Moreover, the capability to develop and integrate a fully interactive and coupled set of national-scale infrastructure models is not being pursued with sufficient priority and support to achieve it in the foreseeable future.

### **Commission-Sponsored Modeling and Simulation (M&S) Activities**

As the Commission embarked on its task, it attempted to engage existing capabilities within academia, industry, and government to simulate the behavior of infrastructures subjected to stressful disruption. To that end, it initiated the following activities.

*National Workshop.* The EMP Commission sponsored a national workshop on the modeling and simulation of interdependent interacting infrastructures as part of an effort to understand the state of modeling capability in this country and to identify capabilities that might be exploited to provide insight into the expected effects of a prescribed EMP attack scenario. A number of national experts who are working on related modeling and simulation activities participated. The Commission has exploited some of these capabilities to develop insight that helped inform the assessment provided by the Commission's full report.

*Contractual Activities.* Current modeling and simulation tools are not sufficient to provide a realistic predictive capability for the interdependent infrastructures. Nevertheless, the modeling capability proved useful in developing the Commission's insight into the effects of coupling on the overall impact due to the attack and the expected recovery and restoration effort. The Commission examined such questions as: Does a strong or weak coupling tend to drive the models to longer or shorter infrastructure restoration times? What seemed to be the sensitive parameters? What sorts of decoupling activities might be suggested to shorten reconstitution efforts? The examination of these and similar questions was supported by a number of efforts the Commission initiated with the NISAC, the University of Virginia, and Argonne National Laboratory. Some of the results of these efforts are summarized in the following section.

*EMP Commission Staff Analyses.* The EMP Commission staff also developed analytic products to explore issues of stability and instability related to infrastructural coupling models. In particular, the Commission focused on models that coupled the power to the telecommunication infrastructure in an interactive way.

The results of these efforts have informed the Commission's findings, as documented in this volume.

### ***Illustrative Modeling and Simulation Results for Coupled Infrastructures***

To illustrate some of the complex behavior that can arise when coupling between infrastructures is included, consider the simple case of the interaction of only two infrastructures, here taken to be the telecommunication and power networks. The telecommunication networks themselves are in the midst of a rapid evolution that has seen data communications, which represented only 10 percent of the total traffic in 1990, grow to about 50 percent of the daily telecommunications load, with the expectation that voice traffic will

---

represent only a small fraction of the traffic by 2015. There is a corresponding ongoing evolution, both in the network architecture and the underlying hardware, that is described in more detail in Chapter 3 of this report.

A critical element of the network of the future will be reliance on public data networks (PDNs). In the past, the electric power grid relied on its own communication system to monitor and control the grid, and mutual dependence between the power and telecommunications systems was essentially nil. Today the power grid relies on PDNs for about 15 percent of its telecommunication needs, and this figure is expected to grow to 50 percent in the near future. **Figure 1-8** illustrates the expected interdependence for this evolving network.

The PDNs represent networks powered by the power distribution network. The power generation and distribution network is, in turn, controlled by SCADA systems that depend on telecommunications to provide situational awareness and to execute control functions for the power grid. **Figure 1-9** represents the results of a model simulation. The telecommunication network reverts back to a dependence on commercial power while both are in the recovery phase. The power infrastructure continues to depend in part on the probability of call blocking, while the recovery for telecommunications depends on the available power.

The figure shows four distinct phases of a recovery process — an early phase extending to about a half hour, during which many network elements execute reinitializations to restore some service with power generally available from battery backup, to a phase of interdependency, during which the only power option left is reliance on the commercial grid, which in turn is dependent on a commercial PDN. This model can provide insight into the recovery process. It predicts significantly lengthened recovery times because of infrastructure interdependency, compared to recovery analysis that examines an infrastructure in isolation, ignoring the factor of interdependency. While illustrative of the effects of interdependency, this model is not meant to represent the actual behavior of any specific real-world system today.

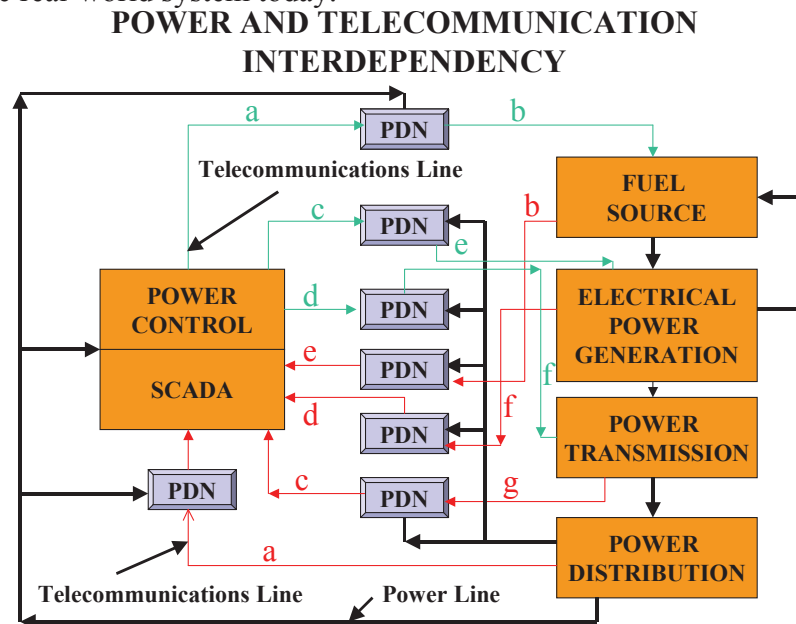


Figure 1-8. Interdependency for Anticipated Network of the Future

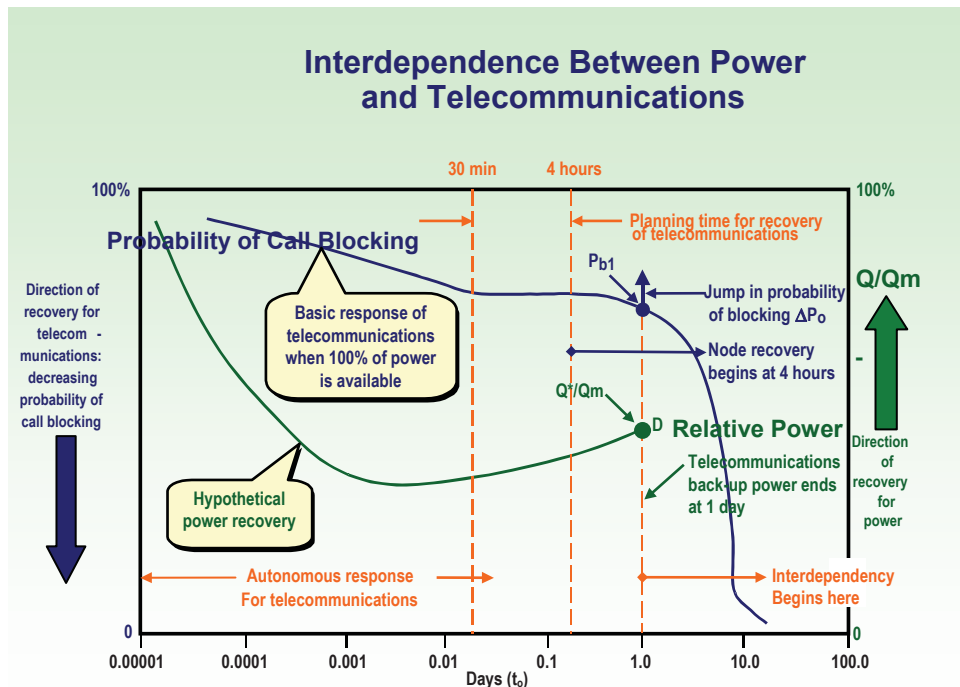


Figure 1-9. Results of a Model Simulation<sup>3</sup>

In another effort, the NISAC studied the consequences of an EMP attack scenario<sup>4</sup> involving a large EMP source located at high altitude off the California coastline. The simulation looked at the effects on water, electric power, telecommunications, natural gas, refined petroleum products, transportation, labor and economic sector productivity and attempted to capture their known interactions. The simulation included network models for the transfer of information and infrastructure products, services, markets, and process models for each product and service. The boundary conditions for the simulation were provided by the EMP Commission; for study purposes, they included descriptions of the potential initial states of both the power and telecommunication infrastructures immediately following exposure to the EMP environment. The simulation, which was not considered realistic because it did not consider likely physical damage that would impede any recovery process, was still useful in providing insight into the potential for disturbances in one infrastructure to cascade into others.

## Summary

No currently available modeling and simulation tools exist that can adequately address the consequences of disruptions and failures occurring simultaneously in different critical infrastructures that are dynamically interdependent. Many infrastructure models that do exist are local to regional in scope.

The Federal Government is supporting a number of initiatives to develop critical national infrastructure modeling and simulation capability as a national analysis and planning resource. However, these are not high national priorities and are funded at less

<sup>3</sup> Kohlberg, Clark, and Morrison, "Theoretical Considerations regarding the Interdependence between Power and Telecommunications," preprint, EMP Commission Staff Paper.

<sup>4</sup> Brown and Beyeler, "Infrastructure Interdependency Analysis of EMP Effects and Potential Economic Losses," EMP Commission Interdependencies Modeling and Simulation Workshop, Washington, D.C., June 2003.



than critical mass. They also are fragmented and uncoordinated, which is not an entirely negative observation, as the complexity of the task merits exploration of independent research and development approaches.

Recent analytic work suggests that evolving interdependencies may be inadvertently introducing entirely new and potentially serious vulnerabilities that could lead to infrastructure failures, even without the precipitating catalyst of an EMP attack.

### **Recommendations**

- ◆ The Commission recommends that research be conducted to better understand infrastructure system interdependencies and interactions, along with the effects of various EMP attack scenarios. In particular, the Commission recommends that such research include a strong component of interdependency modeling. Funding could be directed through a number of avenues, including through the National Science Foundation and the Department of Homeland Security.
- ◆ The Commission recognizes current interest in protecting SCADA systems from electronic cyber assault. The Commission recommends that such activities be expanded to address the vulnerability of SCADA systems to other forms of electronic assault, such as EMP.

## Chapter 2. Electric Power

### Introduction

The functioning of society and the economy is critically dependent upon the availability of electricity. Essentially every aspect of American society requires electrical power to function. Contemporary U.S. society is not structured, nor does it have the means, to provide for the needs of nearly 300 million Americans without electricity. Continued electrical supply is necessary for sustaining water supplies, production and distribution of food, fuel, communications, and everything else that is a part of our economy. Continuous, reliable electrical supply within very tight frequency boundaries is a critical element to the continued existence and growth of the United States and most developed countries.

For most Americans, production of goods and services and most of life's activities stop during a power outage. Not only is it impossible to perform many everyday domestic and workplace tasks, but also people must divert their time to dealing with the consequences of having no electricity. In the extreme, they must focus on survival itself. The situation is not different for the economy at large. No other infrastructure could, by its own collapse alone, create such an outcome. All other infrastructures rely on electric power. Conversely, the electric power infrastructure is dependent on other infrastructures that are themselves vulnerable to the direct effects of electromagnetic pulse (EMP) in ways that are described elsewhere in this report. No infrastructure other than electric power has the potential for nearly complete collapse in the event of a sufficiently robust EMP attack. While a less robust attack could result in less catastrophic outcomes, those outcomes would still have serious consequences and threaten national security.

The electrical power system is the largest single capital-intensive infrastructure in North America. It is an enormously complex system of systems containing fuel production, gathering and delivery systems, electrical generators (often themselves systems), electrical transmission systems, control systems of all types, and distribution systems right down to the electrical outlet and interconnection at the point of use. It is this vast array of systems and components all acting in concert, integrated into a cohesive whole to deliver electrical power at the point of use, with supply-on-demand at a uniform frequency that provides the reliable, steady, and adequate electric supply on which everyone has come to expect and depend. Because of the integration and interdependence of the electric system's components and the ever growing shift to electronics and particularly microelectronics for operation, protection and control, the Nation is particularly vulnerable to a major disruption of the electric supply.

Today, the existing electrical system at peak demand periods increasingly operates at or near reliability limits of its physical capacity. Modern electronics, communications, protection, control and computers have allowed the physical system to be utilized fully with ever smaller margins for error. Therefore, a relatively modest upset to the system can cause functional collapse. As the system grows in complexity and interdependence, restoration from collapse or loss of significant portions of the system becomes exceedingly difficult. Over the last decade or two, relatively few new large-capacity electric transmission capabilities have been constructed and most of the additions to generation capacity that have been made have been located considerable distances from load for environmental, political, and economic reasons, adding stress and further limiting the system's ability to withstand disruption. Significant elements of the system, including many generating plants, are aging (a considerable number are more than 50 years old)



and becoming less reliable or are under pressure to be retired for environmental considerations, further exacerbating the situation.

Should the electrical power system be lost for any substantial period of time, the Commission believes that the consequences are likely to be catastrophic to civilian society. Machines will stop; transportation and communication will be severely restricted; heating, cooling, and lighting will cease; food and water supplies will be interrupted; and many people may die. “Substantial period” is not quantifiable but generally outages that last for a week or more and affect a very large geographic region without sufficient support from outside the outage area would qualify. EMP represents such a threat; it is one event that may couple ultimately unmanageable currents and voltages into an electrical system routinely operated with little margin and cause the collapse of large portions of the electrical system. In fact, the Commission is deeply concerned that such impacts are certain in an EMP event unless practical steps are taken to provide protection for critical elements of the electric system and to provide for rapid restoration of service, particularly to essential loads.

The electrical power system routinely experiences disruptions. In most cases, the cause is the failure of one or a small number of components. The overall system has a degree of durability against such failures, although in some cases failures lead to a cascading loss of power up to a regional level that extends over relatively short to moderate periods of time. The current strategy for recovering from such failures is based on the assumption of sporadic failures of small numbers of components, and for larger failures, drawing on resources from outside the affected area. This strategy leaves us ill-prepared to respond effectively to an EMP attack that would potentially result in damage to vast numbers of components nearly simultaneously over an unprecedented geographic scale.

The Commission recognizes that EMP is one of several threats to the overall electrical power system. Some of these threats are naturally occurring, such as geomagnetic storms. Others, like attacks using information operations on the system’s controls, are manmade. There are strong similarities in the types of damage resulting from the occurrence of such threats. There are also similarities in the measures that are appropriate to be undertaken to reduce the electrical power system’s vulnerability to each of these threats. The Commission believes that the measures it recommends will both reduce the vulnerability of the electrical power system to these threats and improve the Nation’s ability to recover the system.

The magnitude of an EMP event varies with the type, design and yield of the weapon, as well as its placement. The Commission has concluded that even a relatively modest-to-small yield weapon of particular characteristics, using design and fabrication information already disseminated through licit and illicit means, can produce a potentially devastating E1 field strength over very large geographical regions. This followed by E2 impacts, and in some cases serious E3 impacts operating on electrical components left relatively unprotected by E1, can be extremely damaging. (E3 requires a greater yield to produce major effects.) Indeed, the Commission determined that such weapon devices not only could be readily built and delivered, but also the specifics of these devices have been illicitly trafficked for the past quarter-century. The field strengths of such weapons may be much higher than those used by the Commission for testing threshold failure levels of electrical system components and subsystems.

Additionally, analyses available from foreign sources suggest that amplitudes and frequency content of EMP fields from bomb blasts calculated by U.S. analysts may be too low. While this matter is a highly technical issue that awaits further investigation by U.S. scientific experts, it raises the specter of increased uncertainty about the adequacy of current U.S. EMP mitigation approaches.

A key issue for the Commission in assessing the impact of such a disruption to the Nation's electrical system was not only the unprecedented widespread nature of the outage (e.g., the cascading effects from even one or two relatively small weapons exploded in optimum location in space at present would almost certainly shut down an entire interconnected electrical power system, perhaps affecting as much as 70 percent or possibly more of the United States, all in an instant) but more significantly widespread damage may well adversely impact the time to recover and thus have a potentially catastrophic impact.

For highly dependent systems such as commercial telecommunications and the financial system, electric power is frequently filtered through batteries. These act to condition the power as well as to provide limited backup. Local, at-site emergency generators are used quite extensively for high priority loads. These include hospitals, cold storage, water systems, airport controls, rail controls and similar uses. These systems, however, are themselves increasingly dependent on electronics to initiate start up, segregate them from the larger power system, and control their operating efficiency, thereby rendering them vulnerable to EMP.

Furthermore, emergency generators have relatively short-term fuel supplies, generally less than 72 hours. Increasingly, locally stored fuel in buildings and cities is being reduced for fire safety (after 9/11) and environmental pollution reasons, so that emergency generation availability without refueling is becoming even more limited. Batteries normally have a useful life well short of emergency generators, often measured in a few hours. All of these tools for maintaining a stable and adequate power supply, even to high priority loads, are intended to be temporary at best – bridging the time until restoration can take place.

The impact of such an EMP-triggered outage would be severe but not catastrophic if the recovery was rapid or the geographic impact sufficiently limited. The recovery times from previous large-scale outages have been on the order of one to several days. This record of quick recovery is attributable to the remarkably effective operation of protective systems and communications that are an essential part of the power infrastructure and the multiple sources of replacement components from surrounding nonimpacted systems. In this context, a short blackout scenario over a relatively small geographic region would be economically painful. Of the more than \$10 trillion U.S. Gross Domestic Product, about three percent is electricity sales. However, estimates of economic loss from historical blackouts range from factors of six (for domestic customers) to 20 (for industrial users) times the value of the interrupted service. By these measures, the economic impact of an outage is between 18 and 60 percent of total production in the affected area. Again, this estimate is for reasonably short-lived blackouts. A short blackout presents no threat to national survival.

On the other hand, a geographically widespread blackout that involves physical damage to thousands of components may produce a persistent outage that would far exceed historical experience, with potentially catastrophic effect. Simulation work sponsored by the

---

Commission at the National Infrastructure Simulation and Analysis Center (NISAC) has suggested that, after a few days, what little production that does take place would be offset by accumulating loss of perishables, collapse of businesses, loss of the financial systems and dislocation of the work force. The consequences of lack of food, heat (or air conditioning), water, waste disposal, medical, police, fire fighting support, and effective civil authority would threaten society itself.

The Commission solicited technical assistance and judgment from the North American Electric Reliability Corporation (NERC, which is governed by the Federal Energy Regulatory Commission [FERC] guidelines); utilities with particularly relevant experience (such as with geomagnetic storms [similar to E3]; long or very high voltage transmission; uniquely sensitive generation, special fault testing; and similar aspects); suppliers of protection, control, and other related equipment; groups dealing with industry standards; organizations of utilities, fuel suppliers, fuel transportation groups; select academic, national, and internationally recognized experts, the Department of Energy (DOE) National Laboratories, and relevant governmental entities. Willingness to be helpful was uniformly positive and generous. The Commission is grateful for this support.

NERC was uniquely well suited to be of assistance. NERC was established in the aftermath of the 1965 Northeast Power Failure to enhance the reliability of the electrical system. The Commission briefed the NERC Board of Trustees on the nature of the threat and the potential vulnerability. The NERC Board established an EMP task force under the aegis of its Critical Infrastructure Protection Advisory Group to provide technical advice to the Commission. The expertise of the task force membership spanned the three NERC Interconnects (Eastern, Western States Coordinating Council [WSSC], and Electric Reliability Council of Texas [ERCOT]), and all three major categories of the system (generation, transmission, and distribution).

This group's involvement was an essential element in focusing the Commission on the importance of the early-time EMP pulse and its implications for recovery, as well as on other triggers of widespread impact. It also provided technical input that was very helpful in implementing and interpreting a Commission-sponsored test program targeted at identifying the threshold at which significant control and protective components for the electrical system would begin to fail through disruption, false data, and damage. Many of the technical and operational insights discussed within the report were influenced by this task force although the NERC Task Force did not otherwise directly participate in the drafting of the report or in its conclusions.

## Description

### **Major Elements**

There are three major elements of the electrical power infrastructure: (1) generation, (2) transmission (relatively high voltage for long distances), and (3) distribution, whose elements are interdependent, yet distinct (see **figure 2-1**).

**Generation.** Power plants convert energy that is in some other form into electricity. The initial form of the energy can be mechanical (hydro, wind, or wave), chemical (hydrogen, coal, petroleum, refuse, natural gas, petroleum coke, or other solid combustible fuel), thermal (geothermal or solar), or nuclear. Power plants can range from single solar cells to huge central station complexes. In most circumstances the first stage of generation

converts the original form of energy into rotational mechanical energy, as occurs in a turbine. The turbine then drives a generator.

## Power System Overview

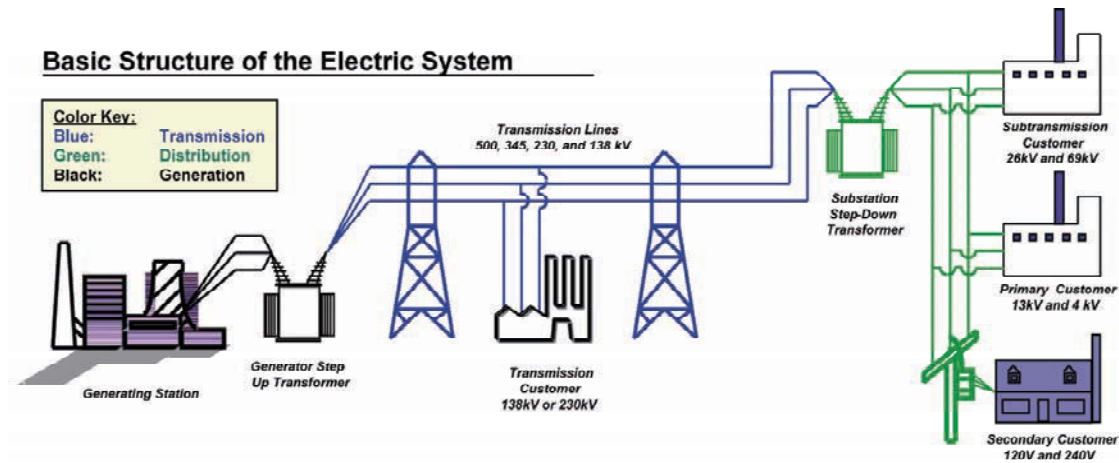


Figure 2-1. Power System Overview

Modern power plants all utilize complex protection and control systems to maximize efficiency and provide safety. They all have common electrical characteristics in order for them to be useable by all the various purposes to which electricity is put. Electronics have largely replaced all the electromechanical devices in older plants and are used exclusively in plants of the past one or two decades. Even generator exciters now have microprocessors and analog-to-digital converters. These electronics and, thus, the power plant itself are highly vulnerable to EMP assault. Identifying and locating damaged generation plant equipment with electronic sensors and communication interdicted and/or unreliable due to EMP and repairing the system would be a complex and time-consuming process, even when personnel and parts are readily available.

The fossil fuel supply system (coal, oil, wood, and natural gas) is largely dependent on electronics for its production and delivery of adequate fuel to the generators to produce nearly 75 percent of the Nation's electricity. There should not be a direct and immediate impact on the fuel supply for a nuclear power plant. The interdependency between the fuel necessary to generate electricity and the electricity and electronics to deliver the fuel is critical to the recovery. For example, natural gas normally is delivered just in time while oil and coal have some at-site storage. Nuclear generation supplies a major portion of the remainder of the Nation's electricity. It is unlikely for the timing of an EMP attack to be such that it would directly and immediately impact the fuel supply for a nuclear power plant. Of the balance, hydroelectric plants have their own fuel supplies as do geothermal, solar, and wind systems. However, wind and solar may or may not be generating in any event, given their inherent uncertainty. Hydro and geothermal are significant capabilities, but they are highly localized.

**Transmission.** Electrical power from the various power plants travels over a system of lines and substations to the regions and locales where it will be consumed. The transmission system moves large amounts of power generally over substantial distances and/or to directly serve very large electrical loads. This definition separates it from the distribution system, which is described below. Transmission includes lines (wires strung from insu-

lator strings on towers or underground in special insulated containers) and substations (nodal points where several lines intersect and protection and control functions are implemented). Within substations there are transformers (which transform power from one voltage to another); breakers (similar to on-and-off switches able to handle the large amounts of energy passing through); and protective devices, meters, and data transmitting and control systems. Protective devices protect the electrical components from unusual electrical disturbances that occur from time to time for many different reasons as well as for general safety reasons.

The delivery of electrical power across or through some medium, such as a wire, encounters resistance, which itself takes power to overcome. Electrical power is measured by the product of voltage and current. The electrical resistive losses (restricting the flow) are proportional to the square of the current. Thus it is most efficient to transmit power at the minimum current that is practical (this results in the highest voltage for the same amount of power). Otherwise, more power is consumed just to push the electricity through or over a path with higher resistance.

Standard values for modern alternating current (AC) transmission line voltage range from 115 kV (115 thousand volts) to 765 kV, although some 1100 kV transmission has been developed and tested. The current carried by these lines is typically up to a few thousand amperes. Direct current (DC) is also used in some instances for moving large amounts of power great distances and for controlling the flow itself. The normal point of use of electricity is AC and thus the shift from AC to DC and back from DC to AC makes DC uneconomical other than in special circumstances. The use of DC is increasing, however, as power costs continue to grow and the technology to shift from AC to DC and back becomes less expensive. Transformers within the substations are used to move the voltage from one line or power plant up to or down to another voltage while maintaining essentially the same level of power.

***Distribution.*** Loads or end users of electricity (residences, commercial establishments, and even most industry) require electrical power to be available in the voltages needed in adequate supply when they need it. This often means in relatively small quantities at low voltage and current. The size of the wires and switches in a typical house are able to be quite small and of much lower cost because the power available to that house is restricted to be relatively low. The electrical and electronic appliances similarly need only a small amount of power to be available. Therefore, the high-voltage power of the transmission system described previously is reduced (stepped down) through transformers and distributed to the end users in levels they need and can use. Reactive load balancing equipment is also part of the distribution system. This equipment is needed for system stability. The electrical power system's stability is finely tuned and fragile. Large-scale failures most often occur because the system is destabilized by local anomalies.

The distinction between transmission and distribution is sometimes a fuzzy one because it depends on the size and need of the load and the specific system involved. The distinction is relevant for regulatory and business purposes. It does vary somewhat from region to region. Traditionally distribution distances are under 20 miles and voltages are less than 69.5 kV (more commonly 13.5 kV). However voltages up to 115 kV are used in some locations. Distribution has substations just like transmission, only smaller. These are not manned. Of importance is that the local switching, controls, and critical equipment have become largely electronic with concomitant vulnerability to EMP.



Alternating current, as opposed to direct current, is the medium for use of electricity as a general matter. Electricity production, transmission, distribution, and use require a precise frequency. Thus it is necessary across the vast electrical power system to precisely and reliably synchronize the frequency and phase of power coming from different generating sources and reaching and being utilized by different loads. Testimony to the accuracy of this control has been the wide use and dependence on electric clocks and the functioning of many electronic devices. The difficulty of maintaining the frequency synchronization during off-normal conditions is usually a factor in large-scale power outages. For example, when the frequency moves very far from a constant required level, protective schemes at the generators within the transmission system and at the loads alarm and often automatically trip. Occasionally these trip out of proper sequence causing the system to compound rather than mitigate the problem, and the system collapses.

*Control and Protection Systems.* Overlaid on these three primary elements — generation, transmission and distribution — is a control system that directs the power where it is needed, maintains the frequency, and protects the system. Control is also necessary for commercial aspects. The controls must protect the system from transients such as lightning, correct synchronization errors by activating reactive sources or loads, isolate malfunctioning elements of the grid, and prevent self-damage from improper compensation or human error. The control systems also enable the deregulated energy marketplace by tracking the origin, route, and destination of the energy commodity. Central to the monitoring and coordination of the power grid is a broad class of devices called supervisory control and data acquisition (SCADA) systems. These conform to an agreed set of standards that make it possible to network many such systems over a generic communications system, regardless of modality. SCADA devices are in broad use in a variety of applications other than power.

The revolution in communication, information, system and component protection, and control technologies has reached essentially every segment of the economy, and its heavy impact on the electric power industry is no exception. The growing dependence of our infrastructures on ubiquitous electronic control and protection systems confers great benefits in terms of economic and operational efficiency, rapid diagnosis of problems, and real-time remote control. At the same time and less often remarked, it also represents a potential new vector of vulnerability that could be exploited by determined adversaries, and intellectual efforts to mitigate such threats have been engaged. The infrastructure's vulnerability to EMP and other broad-impact events raises the threat to an entirely new and vastly expanded plane of serious to catastrophic impacts.

Electronics have enabled electric power systems — generation, transmission, and distribution — to achieve greater levels of efficiency and safety with much lower adverse environmental impacts. Far less generation, transmission, and distribution are now necessary to provide the same amount of benefit to the end user, thus significantly enhancing productivity and overall quality of life. In doing so, however, the electrical system operates closer to theoretical capacity and thus at narrower margins of safety and reliability. Electronics have improved system economics and lowered the overall cost of power to the end user while reducing pressure on basic resources and limiting potential adverse impacts on the environment. This enhanced capability, both on the provider and consumer side, is in part responsible (along with the regulatory environment) for the low rate of investment in the high-value components of the electric system infrastructure. For



example, slowly increasing electrical transmission demand has largely been met within the limits of current production capacity for these components.

The continuing evolution of electronic devices into systems that once were exclusively electromechanical, enabling computer control instead of direct human intervention and use of broad networks like the Internet, results in ever greater reliance on microelectronics and thus the present and sharply growing vulnerability of the power system to EMP attack. Just as the computer networks have opened the possibility to cyber assault on the power system or to electrical power system collapse associated with software failure (as during the August 14, 2003, blackout), they have provided an opportunistic pathway for EMP attack that is likely to be far more widespread, devastating, and difficult to assess and restore. Switches, relays, and even generator exciters now have microprocessors and analog-to-digital converters. These and other low-power electronics cannot be expected to withstand EMP-generated stresses unless they are well protected. Protection must encompass both device design and system integration. Even a well-designed system installed without regard for EMP intrusion via connecting lines can be rendered inoperative by EMP stress. There is a serious question regarding whether manual control of the system sufficient to allow continued service will be possible even at a much-reduced state in the aftermath of EMP.

The key vulnerable electronic systems are SCADA along with digital control systems (DCS) and programmable logic controllers (PLC). SCADAs are used for data acquisition and control over large and geographically distributed infrastructure systems while DCSs and PLCs are used in localized applications. These systems all share similar electronic components, generally representative of components that form the internal physical architectures of portable computers. The different acronyms by which we presently identify SCADA, DCS, and PLC should not obscure the fact that the electronics have evolved to the point where the differing taxonomies are more representative of the functional differences of the electronics equipment rather than differences in the electronics hardware itself.

Electronic control equipment and innovative use of electronic controllers in equipment that is not usually considered control equipment are rapidly replacing the purely electromechanical systems and devices that were their predecessors. The use of such control equipment is growing worldwide, and existing users are upgrading equipment as new functionalities develop. The U.S. power industry alone is investing about \$1.4 billion annually in new SCADA equipment. This is perhaps 50 times the reinvestment rate in transformers for transmission. The present rate represents upgrade and replacement of the protection and control systems to ever more sophisticated microelectronics at roughly 25 to 30 percent annually, with each new component more susceptible to EMP than its predecessor. The shift to greater electronic controls, computers, and the Internet also results in fewer operators and different operator training. Thus the ability to operate the system in the absence of such electronics and computer-driven actions is fast disappearing. This is almost certain to have a highly deleterious effect on restoring service in the event of an EMP attack.

### ***Electrical System Organization***

The integrated electrical power system of the United States and integrated systems in Canada and Mexico are covered by the NERC. This vast network is broken into only three truly separate systems at the present time — the Eastern Interconnection, the

---

Western Interconnection, and Texas. The dividing line geographically between the Eastern and Western systems is roughly a line between Montana and North Dakota continuing southward. The largest of these, the Eastern Interconnection, serves roughly 70 percent of the electrical load and population of the United States. The three regions are separated electrically in AC in order to provide barriers for transfer of major frequency deviations associated with system separations. This mode of operation between regions is referred to as maintaining frequency independence. Importantly, this also acts as a barrier to EMP-caused system disruption or any other major system disruption and consequent collapse crossing between these three regions.

In **figure 2-2** the map of the three NERC regions shows the divisions geographically and the barriers for transfer of major frequency deviations associated with system separations. There are some nonsynchronous connections, such as DC back-to-back converter installations that facilitate limited power transfers yet maintain a barrier. The subregions identified in the map within a region are for organizational, record keeping, and management only. They do not have frequency independence from one another at this time. Thus at present, whole regions can be caused to collapse by sufficiently large electrical disturbances, like EMP, which severely exacerbates the problem of service to critical loads and importantly impedes restoration where delay increases the adverse impacts virtually exponentially.

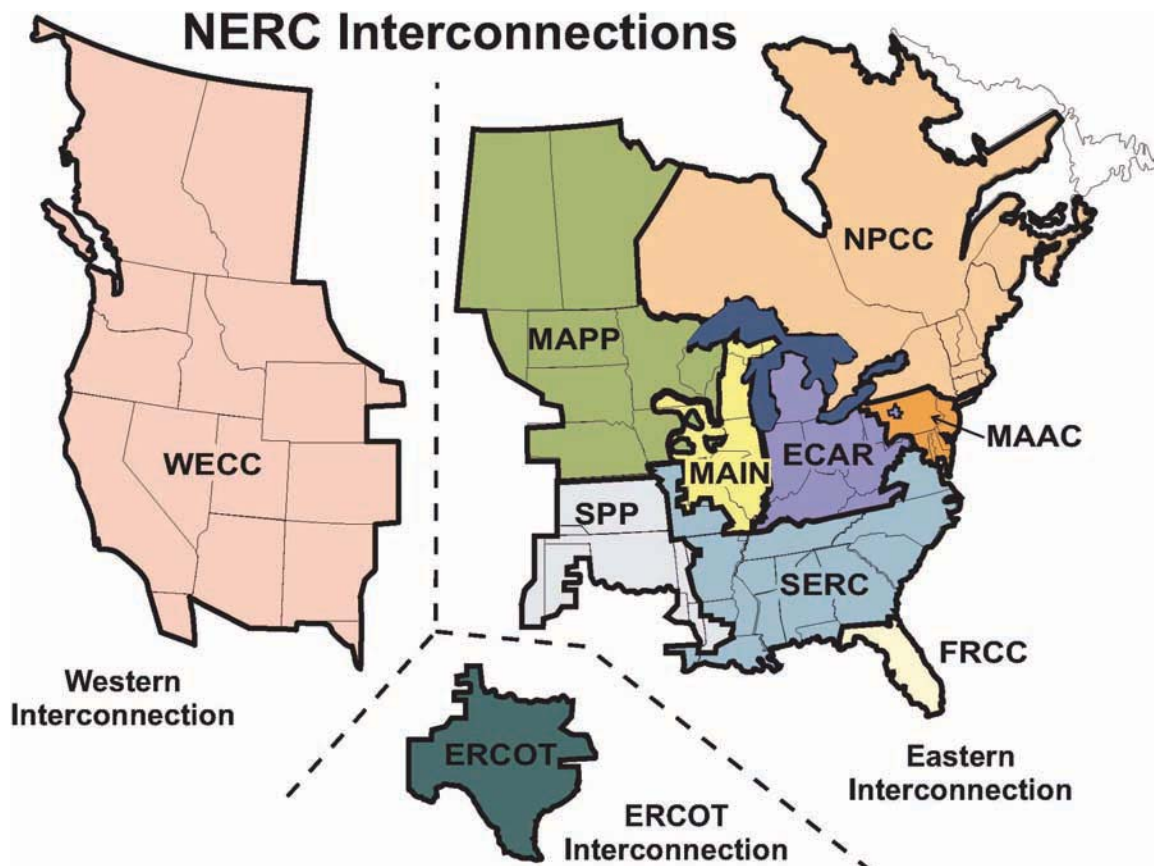


Figure 2-2. NERC Interconnections

### Capacity Reserves

Although greater conservation and efficiency at the end user has reduced the need for new generation largely through the use of improved electronics and controls, the growing

economy and use of ever greater labor- and material-saving devices continues to drive the need for new generation. Furthermore, older generation is being replaced for economic, environmental, and locational reasons. Increasing capital costs emanating from world market competition and natural disasters, plus the increasing cost of capital, have slowed the addition of new generation capacity. The inability in many cases to get generation to market with reasonable assurance due to limited transmission has similarly limited new generation additions. Finally, regulatory returns and pressure from competing uses of capital within utility systems or their parents, including municipal and public systems, have further restricted new generation of consequence. As a result, generation capacity margins have decreased.

Changes in the regulatory environment with greater deregulation of the generating sector have further encouraged recent increases in new generation capacity along with retirement of older units. Most of the new power plants over the past decade or two have been natural gas-fired units that are agile in their ability to adapt to market demands and opportunities, are relatively clean environmentally for fossil plants, faster to build and have lower capital cost than many alternative generator options. They have been located farther from load in most instances than the older plants or previously planned additions, and they are operated and integrated very differently than in the past as economic decisions are often driven by very diverse and nonintegrated responsibility. This can stretch the ability of the transmission system to get the new generation to load. The type and location of new generation stresses the system and increases its vulnerability to various threats including EMP.

The capacity margin (standby capacity for emergencies or other unplanned needs) for the transmission system grid (system of higher voltage lines and substations) has decreased from about 20 percent twenty years ago to about 10 percent now as an overall system matter although there are considerable regional or local variations. This reduced margin is due to little new construction, improved efficiency of the existing system, and the location of new generation away from load. It is further exacerbated by the addition of significant generation from renewable resources such as wind energy, which operates when the wind blows, not when the electrical system might otherwise require power. This results in shifting the generation between the wind and other controllable generation on an unpredictable basis regardless of the transmission system reliability needs, all of which results in greater and less predictable stresses on the overall system.

Operation of the transmission system at today's reduced margin while maintaining excellent reliability has been enabled by improved technology and operating practices for protection, command, and control of the transmission grid. While power production and consumption have grown, almost all of the growth has been absorbed on existing power lines although new substations have been added. There has been very little construction of transmission capacity, particularly of new longer distance transmission lines, or renewal and replacement of existing infrastructure for many reasons, including deregulation (discussed in the next section of this chapter). The transmission system thus is operating with little ability to absorb adverse electrical impacts.

Overall, as a result of reduced generation capacity margins, the generation component of the system is far less able to compensate for the difficulties that may be encountered within the transmission system and vice versa. Together, the consequence is a power system far more vulnerable to disruption than in the past, and this vulnerability is increasing.

While greater protection and control schemes have still provided a very reliable system in spite of this, the system is being stressed beyond reasonable limits. The electrical power system has become virtually fully dependent upon electronic systems working nearly flawlessly. The overall system reliability is testimony to the skill and effectiveness of the control systems. However, the lack of margin (combination of generation and transmission margins) results in making catastrophic cascading outages far more likely, and should the electronics be disrupted, the system is highly likely to fail on a broad scale. Thus, the small margin and reliance on electronics give rise to EMP vulnerability.

High-value assets (assets that are critical to the production and delivery of large volumes of electrical power and those critical for service to key loads) in the system are vulnerable to EMP through the loss of protection equipment due to E1 and even if E3 levels were not large enough to cause damage. The largest and most critical of these are transformers. Transformers are the critical link (1) between generation and transmission, (2) within the transmission network, (3) between the transmission and distribution systems, and (4) from the distribution to the load.

The transformers that handle electrical power within the transmission system and its interfaces with the generation and distribution systems are large, expensive, and to a considerable extent, custom built. The transmission system is far less standardized than the power plants are, which themselves are somewhat unique from one to another. All production for these large transformers used in the United States is currently offshore. Delivery time for these items under benign circumstances is typically one to two years. There are about 2,000 such transformers rated at or above 345 kV in the United States with about 1 percent per year being replaced due to failure or by the addition of new ones. Worldwide production capacity is less than 100 units per year and serves a world market, one that is growing at a rapid rate in such countries as China and India. Delivery of a new large transformer ordered today is nearly 3 years, including both manufacturing and transportation. An event damaging several of these transformers at once means it may extend the delivery times to well beyond current time frames as production is taxed. The resulting impact on timing for restoration can be devastating. Lack of high voltage equipment manufacturing capacity represents a glaring weakness in our survival and recovery to the extent these transformers are vulnerable. Distribution capability is roughly in the same condition although current delivery times are much less (i.e., limited manufacturing capability, although there is domestic production).

### ***Deregulation***

At least a decade ago, the power systems were owned and operated by vertically integrated utility companies. These entities consisted of investor-owned (owned by shareholders, commonly referred to as private) utilities, utilities that are government constructs (federal, such as the Tennessee Valley Authority, Bonneville Power Administration, and others), consumer-owned cooperatives, municipalities, and entities of the state such as peoples and public utility districts. The different entities were granted monopoly powers for service and were regulated through a variety of mechanisms including self-regulation for some of the government entities. In any given service territory, the local utility owned the generation, transmission, and distribution and was responsible for adequate supply, reliability, and other aspects of service quality.

This situation has changed. On April 24, 1996, FERC issued Orders 888 and 889, which encouraged wholesale power supply competition, deregulating this single aspect of



the electrical industry. This allowed any party to produce and sell power to any other party at the wholesale levels (meaning sales to utility or load-serving entities, as opposed to direct retail sales to end users). Existing generation by investor-owned utilities was forced to be divested in many circumstances. This regulation applied only to the investor-owned utilities comprising a bit more than half the total U.S. electrical load. Many governmental or public entities did not possess generation of their own, and some that did followed by example and market imperatives. In some instances states have carried the deregulation further to a variety of forms of competition at the retail level.

The transmission infrastructure has remained regulated, and the previous vertically integrated systems in many instances were not allowed to commercially control their transmission in order to free up competition at the wholesale levels. Due to the complexity of an open market using an infrastructure that was built for another operating environment, the requirements for investment in the transmission system have been uncertain and more expensive. FERC regulates the transmission facilities in terms of use and pricing, but not location. The federal transmission regulation paradigm is moving toward being market based, which will have unknown impacts but is believed to assist in the development of new transmission facilities. The states also play an important role in the regulation of transmission and generation that is not consistent from state to state. With the market (and the market model itself) in flux, there is unwillingness presently to invest in transmission infrastructure.

There is no incentive for the states or localities to accede to construction of lines that are to move power over or through the state or locality without direct benefit to such state or locality. The power going through the lines pays no fees and no taxes to the hosts, although there are minor property taxes on the physical facilities in some instances. Until recently there was no capability to track the path of a given unit of energy when operating in AC and even then it is more calculation via model-specific than actual measurement. This is because AC power travels over the path of least resistance not as the flow of power might be contracted. Thus while a new interconnected line may appear to carry power pursuant to a contract for delivery between two parties, it is unlikely that the power will flow physically as envisioned. Thus it is unclear who will pay for the use of the new line. While new capability to track AC power (E-tags) could provide the basis for fiscal incentives for new line construction, it is not yet widely deployed nor well understood or accepted. Moreover, regulatory requirements create impediments to new line construction even if the incentives and capital are at hand. In short, from a business perspective, transmission lines are often low return or loss centers in the current environment.

The end state of the regulatory paradigm is still undetermined, and this uncertainty coupled with lack of local benefits when passing through state and local areas all contribute to the diminishing transmission capacity margins. There is uncertainty whether, by the time construction of new lines is completed, the investment could be recovered. It is likely that this situation will persist until the market model is clarified and implemented, which may take several years given the complexity and number of competing interests, including between the states and the Federal Government as well as with neighboring states. The market and system reliability pressure may move this faster as recognition and evidence mount. As noted earlier, the reduced and diminishing margins contribute significantly to EMP vulnerability.

## Vulnerabilities

In order to assess the nature of EMP effects on the electrical system, we separately analyzed the potential effects of an electromagnetic pulse on each of the three main constituents of the power system — generation, transmission, and distribution. Within the context of a principal finding of the NERC EMP task force, recovery following an EMP-caused outage within any reasonably acceptable time is contingent largely on preventing damage to the high-value assets (assets that are critical to the production and delivery of large volumes of electrical power and those critical for service to key loads) and identifying and replacing ones that become damaged. Therefore, the Commission focused on identifying what those high value assets might be and their susceptibility to EMP damage. Thus, proper design, installation, and functioning of the protective equipment for these assets during an EMP attack are critical. There are other critical aspects to recovery that are discussed subsequently.

### Generation

A power plant is designed to protect itself in the event of instantaneous loss of load, electrical faults or trips on the interconnected transmission system or internally, frequency excursions beyond rather tight limits, and often for the loss of an external power source for proper shutdown. None of these conditions should damage a power plant if the protective systems function properly, as frequently has been demonstrated. Very little damage to generation has occurred in previous blackouts, including the August 14, 2003, blackout. However, some malfunctioning in the multiple controls throughout a power plant does occur, albeit rarely. Therefore, on a broad enough scale, as in an EMP attack affecting many power plants at once, damage to a small number of these power plants would be expected statistically. Since E2 and E3 are not assessed as direct threats to the generation system (except for their step-up transformers and associated breakers), the critical vulnerability question is E1-induced plant control system failure.

The E1 pulse can upset the protection and control system, including damaging control and protective system components, and cause the plant to trip or trigger emergency controlled shut down. Current, temperature, pressure, frequency, and other physical parameters are monitored by the control systems. These provide independent measurements of same system, and all can cause the plant to trip off line and go to controlled shut down. Given the redundancy of protective system design, either several protective devices or devices in the critical path would have to fail in order for the plant not to initiate protective shutdown. However, if the control system itself or secondary nodal controls and receivers critical to orderly shut down are themselves damaged, as is reasonably possible with E1, then the plant is seriously at risk. Power plants, particularly newer ones, are highly sophisticated, very high-speed machines, and improper shut down can damage or destroy any of the many critical components and can even cause a catastrophic failure. Nuclear plants are an exception due to the nature of their protection schemes.

Given the range of potential E1 levels, analysis and test results provide a basis to expect sufficient upset to cause a plant's system to shut down improperly in many cases. Proper shutdown depends on synchronized operation of multiple controllers and switches. For example: coal intake and exhaust turbines must operate together or else explosion or implosion of the furnace may occur. Cooling systems must respond properly to temperature changes during shut down or thermal gradients can cause boiler deformation or rupture. Orderly spin-down of the turbine is required to avoid shaft sagging and blades impacting the casings. Bearings can easily fail and freeze or damage the shaft if the shut

---



down does not engage emergency lubrication. There are similar issues inside very complex machines operating at high temperatures at fast speeds with tight tolerances. Thus, power plant survivability depends on a great many protective systems creating multiple pathways to plant damage and failure.

Restoration of some damage can be very long term, certainly months and in some instances years. The loss of generation of any size itself would contribute to systemwide collapse and certainly would limit restoration. Manufacturers of generation plant protection and control equipment performed some limited evaluation and while there are layers of redundancy, as noted, more and more these systems are going to computer-controlled microelectronics, and thus are more susceptible to EMP disruption.

At the device level, power plant protective systems are less exposed than the corresponding systems in the transmission grid. They act on local information, so failure of telecommunications systems is not as much of an issue for plant protection where operators are available in most instances 24/7 and can independently assess the situation and act. The control equipment, protective systems, sensors, and current transformers typically (but by no means always) will be inside the plant although this does not necessarily mean they will not be exposed. In general there will be no outside cable runs, so the building itself will provide some EMP protection. However the lengths of these interior cables can be on the order of 100 meters. Cable trays may or may not provide additional protection, depending on their material and installation method. The key is not device- or component-level testing for EMP susceptibility but overall control and protective system test to evaluate vulnerability. Subjecting an entire sophisticated and modern power plant to testing is not feasible. However, it does not take many damaged plants out of the many hundreds to seriously impact the system operation and the ability to restore service. The fact that all power plants exposed to E1 EMP will be illuminated simultaneously (within one power cycle) makes the situation extremely serious.

#### *System Restoration — Generation*

The restoration of the system from collapse is very complex in operation, almost an art rather than a science, and it requires highly trained and experienced operators with considerable information and controls at hand. Basically, in isolated cases or when beginning restoration, a load and generation source has to be identified and interconnected without interference from other loads or generation. These are then matched and gradually restored together. Thereafter, each increment of generation and load is added in turn to a larger operating system of generation and load. As each component of load and generation are included, the frequency will be impacted. If it varies outside very tight limits, it will all trip off and have to be put back together again. In most system disruptions leading to blackouts, there are large amounts of system still intact on the periphery of the disruption, which are able to greatly assist in the restoration, more easily allowing and absorbing each addition of generation and load until all is restored.

Every generator requires a load to match its electrical output as every load requires electricity. In the case of the generator, it needs load so it does not overspin and fail, yet not so much load it cannot function. In a large integrated system, where increments of load and generation are not sufficient to cause the frequency to drop or rise above acceptable margins, it is relatively straightforward and commonplace, just as turning on a lightswitch causes a generator someplace to pick up the load. In the case where the sys-

tem is being restored and there are few loads and generators connected, this matching requires careful management and communication between load and generation.

Generation start-up for most plants requires power from another source to drive pumps, fans, safety systems, fuel delivery, and so on. Some, like hydroelectric and smaller diesels can start directly or from battery sources assuming they can control their access to matching load. In the case of EMP, large geographic areas of the electrical system will be down, and there may be no existing system operating on the periphery for the generation and loads to be incrementally added with ease. Furthermore, recovery of lost generation would be impacted by the loss of other infrastructure in varying degrees according to the type of plant. In that instance, it is necessary to have a “black start”: a start without external power source. Coal plants, nuclear plants, large gas- and oil-fired plants, geothermal plants, and some others all require power from another source to restart. In general, nuclear plants are not allowed to restart until and unless there are independent sources of power from the interconnected transmission grid to provide for independent shutdown power. This is a regulatory requirement for protection rather than a physical impediment. What might be the case in an emergency situation is for the Government to decide at the time.

Black-start generation is that kind of generator that is independent of outside power sources to get started, hence the term black start. Most black start units today are hydroelectric plants, small gas peaking units, small oil-fired peaking units and diesel units. In some cases the black start unit may be collocated with a larger power plant in order to get the larger one started for system restoration. Fuel supply would then be the only issue from the generation perspective; for example, a gas plant might not have the fuel due to EMP damage someplace in the delivery system. Assuming the black start units were not damaged by EMP or have been repaired and assuming they are large enough to be significant, workers can begin the system restoration as building blocks from the generation side of the equation. EI may have also damaged their startup electronics, which will need to be repaired first. It is often the case that generation capable of black start is not manned, so if they fail to start remotely, a person will need to be dispatched to find the problem, locate the needed parts, and get it operating. There are not many black start-capable units in locations that are suitable to independent restoration at this time. Recovery in most regions therefore needs to wait for other areas to restore power and then be reconnected increment by increment.

Even if partially disabled control systems successfully protect the critical generating equipment, all affected plants would face a long process of testing and repairing control, protective, and sensor systems. Protective and safety systems have to be carefully checked out before start up or greater loss might occur. Repair of furnaces, boilers, turbines, blades, bearings, and other heavy high-value and long lead-time equipment would be limited by production and transportation availability once at-site spares are exhausted. While some spare components are at each site and sometimes in spare parts pools domestically, these would not cover very large high-value items in most cases, so external sources would be needed. Often supply from an external source can take many weeks or several months in the best of times, if only one plant is seeking repair, and sometimes a year or more. With multiple plants affected at the same time, let alone considering infrastructure impediments, restoration time would certainly become protracted.

### ***Transmission***

Most generation is located outside major population areas and thus sometimes at great distances from the load being served. In general, electricity often travels great distances on an efficient high-voltage transmission system. The transmission system is made up of different owners, voltage levels, and controls. Yet power must be routed to where it is needed, so there are nodes called substations where the power lines join and are switched, and where power is moved from one voltage level to another level, interconnected with other transmission system components, and sent on to distribution systems. Finally as it gets closer to load, power is stepped down (reduced in voltage) and then down again and often down yet again to and within the distribution system and then normally down again to the delivery point for the load. Each of those step-down points requires a transformer to effect the change and breakers to isolate the transformer when necessary.

In the event of the loss of a generation facility, a fully functional transmission system can move the remaining generation from whatever plants can operate to areas otherwise affected by loss of a particular generating station. This occurs in normal practice as generation plants are brought in and out of service for one reason or another. The same thing happens when part of the transmission system is down for whatever reason. Other transmission in the network picks up the loss and generation is shifted so that the loads can continue to be served. All this is accomplished regularly as part of system operation. The ability to adjust quickly given access to a multitude of resources, generation, and transmission makes the system reliable. Incapacitation of sufficient elements of the transmission system would mean the inability to deliver power whether the generation is available or not. The same inability would be true for incapacitation of sufficient generation. In the case of EMP, both would be likely to be impacted simultaneously. This is what results in a blackout where the load does not get served. The transmission system is highly vulnerable to EMP.

Substation control systems at the nodes or hubs in the transmission system are inherently more exposed to the E1 pulse than their power plant counterparts, which are often not in buildings at all. The sensors, communications, and power connections are outdoors and cables (i.e., antennas in the sense of an EMP receptor) which may be hundreds of meters long may be buried, run along the ground, or elevated. The control devices themselves, including the protective relays, may even be in remote structures that provide little electromagnetic attenuation. Most substations do not have operators present but are remotely controlled from power dispatch centers, in some instances hundreds of miles away.

Operation of transmission substations depends on various communications modalities, including telephone, microwave, power line communications, cell phones, satellite phones, the Internet, and others. Typically, these modes are used for dedicated purposes; they do not necessarily provide a multiple redundant system but are “stove piped.” From the point of view of managing routine system perturbations and preventing their propagation, NERC advises us that the telephone remains the most important mode. If the voice communications were completely interrupted, it would be difficult, but still reasonably possible, to successfully continue operations — provided there were no significant system disruptions. However in the case of an EMP event with multiple simultaneous disruptions, continued operation is not possible. Restoration without some form of communication is also not possible. Communication is clearly critical in the path to restoration.

Just as in the case involving power plants, the first critical issue is the proper functioning of the protective elements, specifically relays, followed by the local control systems. These elements protect the high-voltage breakers and transformers that are high-value assets. High-value assets are those that are critical to system functioning and take a very long time to replace or repair. Other protected devices, such as capacitors and reactive power generators, are also high value and nearly as critical as the transformers. E1 is likely to disrupt and perhaps damage protective relays, not uniformly but in statistically very significant numbers. Left unprotected, as would likely result from E1 damage or degradation to the protective relays, the high-value assets would likely suffer damage by the transient currents produced during the system collapse, as well as potentially from E2 and E3 depending upon relative magnitudes. Commission testing of some typical protective relays with lower than expected EMP levels provides cause for serious concern.

The high-value transmission equipment is subject to potentially large stress from the E3 pulse. The E3 pulse is not a freely propagating wave like E1 and E2, but the result of distortions in the Earth's magnetic field caused by the upper atmosphere nuclear explosion. The distortion couples very efficiently to long transmission lines and induces quasi-direct current electrical currents to flow. The currents in these long lines can aggregate to become very large (minute-long ground-induced currents [GIC] of hundreds to thousands of amperes) sufficient to damage major electrical power system components. With respect to transformers, probably the hardest to replace quickly, this quasi-direct current, carried by all three phases on the primary windings of the transformer, drives the transformer to saturation, creating harmonics and reactive power. The harmonics cause transformer case heating and over-currents in capacitors potentially resulting in fires. The reactive power flow would add to the stresses on the grid if it were not already in a state of collapse. Historically, we know that geomagnetic storms, which can induce GIC flows similar to but less intense than those likely to be produced by E3, have caused transformer and capacitor damage even on properly protected equipment (see **figure 2-3**). Damage would be highly likely on equipment unprotected or partially protected due to E1.



**Figure 2-3. GIC Damage to Transformer During 1989 Geomagnetic Storm**

The likelihood and scope of the E3 problem are exacerbated by the small transmission margins currently available. The closer a transformer is operating to its performance limit, the smaller the GIC needed to cause failure. Moreover, newer transmission substations are increasingly using three single-phase transformers to handle higher power transfer, since the equivalently rated three-phase transformers are too large to ship. The three-phase systems are more resistant to GIC, since their design presumes a balanced three-phase operation. Thus the separate single-phase transformers are more susceptible to damage from GIC.

#### *System Restoration — Transmission*

The transmission system is the lynch pin between generation and load. It is also a network interconnecting numerous individual loads and generating sources. To restore the overall power system to get generation to load, as noted earlier, an increment of genera-



tion needs to be matched to an increment of load and then add the next matching increments and so on. As the number of increments becomes greater, there is some flex in the system to absorb variations. As a result, the restoration is easier and goes much faster. In the initial increments however, the transmission system link between generation and load has to be isolated so other loads, which may well remain connected, do not impact the effort. This is tricky and requires careful coordination to adjust the breakers in the substations so the link is routed correctly and safely.

The power transmission grid is designed to break into islands of hopefully matched generation and load when the system receives a sufficient electrical disruption. This is both to protect service in the nonimpacted regions and to allow for the stable systems to be used to restart the island that lost functionality. With EMP, broad geographic reach and simultaneous multiple levels of disruption result in a situation in which the islanding schemes themselves will probably fail to work in the EMP-affected area. Since the geographic area is so large, perhaps encompassing an entire NERC region or possibly more, restoring the system from the still functioning perimeter may well not be possible at all or would take a great deal of time; the Commission estimates weeks to months, at least in the best circumstance.

### ***Distribution***

Most of the long power outages that Americans have experienced were due to physical damage to the distribution system — local damage. This damage is usually caused by natural events such as weather. Windblown trees fall on neighborhood power lines or ice buildup drops lines that in some instances make contact with live lines causing arcs that in turn can even result in distribution transformers exploding.

EMP damage to the distribution system would be less dramatic than that inflicted upon the transmission system but still would result in loss of load. The principal effect of EMP would be E1-induced arcing across the insulators that separate the power lines from the supporting wood or metal poles. The arcing can damage the insulator itself and in some cases result in pole-mounted transformer explosions. Damage to large numbers of insulators and pole-mounted transformers could also result in a shortage of replacement parts, as these items are fairly reliable under normal conditions, and spares are not kept to cover widespread losses. Ultimately workarounds and replacements can be found in most circumstances although widespread damage and impact to related infrastructures will cause delay.

The important effect of the loss of load in the EMP scenario is that it happens simultaneously. Thus it represents a substantial upset to the entire grid, causing the frequency to spin up and protective relays to open on generation and can by itself result in a cascading failure and blackout of the entire NERC region. Similarly, any consumer or industrial electrical device that is shut down or damaged by EMP contributes to the load loss and further drives the system to collapse. It becomes a case of what comes first to cause what failure since the EMP E1 impulse is virtually simultaneously disrupting all facets of the electrical system and load.

### ***Synergistic Effects of E1, E2, and E3***

The effects of EMP on the electrical power system are fundamentally partitioned into its early, middle, and late time effects (caused by the E1, E2, and E3 components, respectively). The net impact on the electric power grid includes the synergistic interaction of all three, occurring nearly simultaneously over a large geographic area. The

---

Commission has concluded that the electrical system within the NERC region so disrupted will collapse with near certainty. Thus one or more of the three integrated, frequency-independent NERC regions will be without electrical service. This loss is very large geographically and restoration is very likely to be beyond short-term emergency backup generators and batteries. Any reasonable EMP event would be much larger than the Texas region so basically the concern is the Eastern and Western regions with Texas either included or not depending upon the location of the weapon. The basic threat to U.S. society that moves an EMP event from a local or short-term adverse impact to a more prolonged and injurious event is the time it takes to restore electrical and other infrastructure service.

The early time EMP, or E1, is a freely propagating field with a rise time in the range of less than one to a few nanoseconds. E1 damages or disrupts electronics such as the SCADA, DCS, and PLC as well as communications and to some extent transportation (necessary for supplies and personnel). This disrupts control systems, sensors, communication systems, protective systems, generator systems, fuel systems, environmental mitigation systems and their related computers, as well as the ability to repair. SCADA components, in particular, are frequently situated in remote environments and operate without proximate human intervention. While their critical electronic elements are usually contained within some sort of metallic box, the enclosures' service as a protective Faraday cage is inadequate. Such metallic containers are designed only to provide protection from the weather and a modicum of physical security. They are not designed to protect the electronics from high-energy electromagnetic pulses, which may infiltrate either from the free field or from the many antennae (cable connections) that compromise electromagnetic integrity.

The E1 pulse also causes flashovers in the lower voltage distribution system, resulting in immediate broad geographic scale loss of electrical load and requiring line or insulator replacement for restoration.

The intermediate time EMP, or E2, is similar in frequency regime to lightning, but vastly more widespread, like thousands to millions of simultaneous lightning strikes, even if each strike is at lower amplitude than most naturally occurring lightning. The electrical power system has existing protective measures for lightning, which are probably adequate. However, the impact of this many simultaneous lightning-like strike disruptions over an extremely large geographic area may exceed those protections. The most significant risk, however, is synergistic because the E2 pulse follows on the heels of the E1. Thus where E1-induced damage has circumvented lightning protection, the E2 impact could pass directly into major system components and damage them.

The late time EMP, or E3, follows E1 and E2 and may last for a minute or more. The E3 pulse is similar in a great many respects to geomagnetic effects induced by solar storms. Solar storms and their impacts on electrical systems with long lines have been thoroughly evaluated and are known to cause serious damage to major electrical system components at much lower levels than the reasonably possible E3 impact. This damage has been incurred in spite of functioning, in-place protective systems. Given the preceding E1 and E2 pulse damage to the protective systems and other system components, damage from E3 to unprotected major system components is virtually assured.

EMP is inimical to the continued functioning of the electrical power system and the reliable behavior of electronics. Each of the three EMP modes of system insult is suffi-



cient by itself to cause disruption and probable functional collapse of large portions of the interconnected electrical power system at EMP threat levels. In every EMP attack, all three assaults (E1, E2, and E3) are delivered in sequence and nearly simultaneously. It is the Commission's assessment that functional collapse of the electrical power system region within the primary area of assault is virtually certain. Furthermore, widespread functional collapse may result even from a small weapon with a significant E1 component. While stopping electrical supply over a broad geographical area nearly instantaneously is damaging, it is the time it takes to restore service that is important, assuming restoration is possible, which itself may be questioned in some instances.

### **System Collapse Scenarios**

NERC was one of several key advisers on the EMP impact assessment discussed above although the conclusions and emphasis are the Commission's alone. NERC also informed the Commission that there is no modeling capability extant, either deterministic or statistical, that can assess with confidence the outcome of simultaneous, combined subsystem failures. Putting together a coherent picture of the projected system collapse scenario must rely on expert judgment.

Large-scale load losses in excess of 10 percent are likely at EMP threat levels. Instantaneous unanticipated loss of load, by itself, can cause system collapse. This is possible at 1 percent loss, and is very likely above 10 percent. At similar percentage levels, loss of generation can also cause system collapse. Both the load loss (normally from a transmission system failure) and generation loss resulting in system collapse have been experienced. At the levels of loss for each, collapse is highly likely if not certain. Systemwide ground-induced currents in the transmission grid can by themselves cause system collapse. They did so in March 1989 in Quebec. At the levels expected in an E3 event, collapse would be much more likely and widespread.

Loss of computer control of substation switchyard equipment could, by itself, lead to system collapse. Manual operation is possible only with adequate communication and the ability of personnel to physically get to the right substations, a problematic question in the event of an EMP attack. Adequate numbers of trained and experienced personnel will be a serious problem even if they could all be contacted and could make themselves available. Thus manual operation would be necessary and might not be timely enough or have sufficient skilled personnel to deal with a broad-scale, instantaneous disruption and dynamic situation. Loss of manual control of switchyard equipment would, in short order, lead to line and transformer faults and trips. Several substations tripping nearly simultaneously would lead itself to system collapse.

Loss of telecommunications would not, by itself, cause immediate system collapse except as needed to address issues caused by the above disruptions. However the lack of telemetered control data would make the system operators effectively blind to what is going on, but personnel at substations, if they can get there and communicate with the system operators, could overcome much of that. Malfunction of protective relays could cause system collapse by contributing to several of the above scenarios through misinformation or by operating incorrectly.

All of these collapse mechanisms acting simultaneously provide the unambiguous conclusion that electrical power system collapse for the NERC region largely impacted by the EMP weapon is inevitable in the event of attack using even a relatively low-yield device of particular characteristics.

---

### ***Damage Scenarios***

The level of damage depends primarily on the functioning of the protective equipment, but it also depends on various aspects of the collapse. In an EMP event, the collapse is virtually instantaneous. The size of the transients on the system may be greater than existing protective systems are capable of handling, even those not damaged by the EMP itself.

Damage to the large transformers and other high-value equipment is directly related to protective relay failure, although it is possible for E1-induced arcs inside transformers to damage transformers irrespective of relay failure. In general, since sequential shutdown is not required, one device per relay is a reasonable rule of thumb. A properly functioning relay has a reasonable chance of protecting the device; an improperly functioning one will probably result in some level of damage in an ensuing system collapse. The level of damage depends on the failure mode. The Commission-sponsored tests were focused on determining the thresholds for damage. EMP threat levels are expected to exceed these thresholds.

### **Test Results**

The EMP Commission conducted both free-field and cable current injection simulation testing. The Commission took the basic stance in its testing program that testing would determine the thresholds at which substantial failure rates (either temporary or permanent) commenced to appear. These, in turn, were used to index attack severities at which the corresponding U.S. infrastructures would be seriously compromised or failed. The Commission's test experience — massively supplemented by that of other U.S. Government operations — was that failure rates typically increased rapidly with peak field amplitude, once a threshold had been attained at which failure or disruption appeared at all. The rationale for such threshold determining testing was that abrupt and synchronized loss of only a few percent of items such as electric power system relays would have grave impacts on the functionality of the system containing such items. This is much like the effect that a few percent of vehicles on a freeway that become disabled would have, producing a serious deleterious impact on the flow of traffic.

A crude rule of thumb was that roughly a factor-of-ten increase in damage effects might be expected when the peak field amplitude was doubled; the exact scaling relation naturally varied from one device type to another and also had very substantial dependence on the frequency content of the pulse, which however, the Commission testing program explored only slightly.

Based on the testing and analysis outlined in this chapter, we estimate that a substantial and highly significant fraction of all control and protective systems within the EMP-affected area will experience some type of impact. As the test results were briefed to industry experts at NERC and the Argonne National Laboratory, it became apparent to the Commission that even minor effects noted during the testing could have significant impacts on the processes and equipment being controlled.

### ***Free-Field Testing***

EMP free-field simulation testing was conducted using a bounded wave simulator (see **figure 2-4**). The testing was conducted in three phases.

Phase I was dedicated to evaluating the so-called transfer response for the various test systems. This is a measure of the coupling strength of the external perturbation to the test

system and provides insight into the expected fraction of the energy in an EMP field that may be deposited into the exposed electronic device. Induced current transients were measured on all the accessible cables of the control systems and measurements were made at the lowest field levels produced by the simulator to minimize the electrical stress on the exposed equipment. Phases II and III of the testing program were focused on obtaining data on fragilities, that is, on identifying the thresholds for induced malfunction or damage response in the tested equipment. A total of eight steps were selected that



Figure 2-4. EMP Simulator

gradually increased the electrical stress on the control systems. During this testing, all systems were operational with diagnostics and checkouts run at the conclusion of each simulated EMP exposure.

The simulation testing provided an opportunity to observe the interaction of the electromagnetic energy with equipment in an operational mode. Observed effects can be related to the system response in more realistic scenarios through analysis based on coupling differences between the simulated and real-world cases. Since the simulation is not perfect — the pulse length is too long and the test volume too small to capture the longer cable run couplings to be found in a real environment — post test analysis and engineering judgment is required to relate the test results to expected SCADA vulnerabilities in a true EMP event.

There is also no pretense that any test program could possibly do more than selectively sample the wide variety of installed SCADA systems. The choice of representative test systems was guided by findings from previous infrastructure site surveys, by solicited recommendations from industry groups such as the NERC, and by conducting a review of several market surveys.

In the end, four separate control systems were acquired for testing. These systems were representative of those found in power transmission, distribution, power generation, and oil and gas distribution for fueling power plants.

A key observation from this test program is that a wide variety of SCADA, DCS, and PLC malfunctions resulted when exposed to simulated threshold level EMP environments. These ranged from electronic upset of equipment, which might be repaired by

either reboot or recycle to physical damage that required the actual replacement of the affected hardware.

The response of the control systems tested varied from system to system as well as from subsystem to subsystem. For example, a unit consisting of multiple input/output ports (or subsystems) connected to a variety of field or communications devices had some ports experience upsets, some experience physical damage, and some experience no effect, all in the same simulation event.

As an example, at relatively low electromagnetic stress levels, a portion of a DCS process controller provided false indications of the process status. An operator interface indicated a switch was on when in actuality it had been turned off, while internal voltage and temperature were reported as out of their normal operating ranges when they were actually normal. These effects were significant because they occurred most frequently on control systems used in SCADA applications, which are geographically dispersed. Correcting these malfunctions typically had to be performed manually at the device location. This approach would greatly complicate the recovery process for geographically distributed systems.

In addition to false readings from the sensors, direct malfunctions of some tested control elements were also noted. Additional control element effects included the failure of pressure transmitters, which included both physical damage and loss of calibration data required to indicate proper readings.

Control systems often rely on Ethernet for communications to the man-machine interface as well as communications between controllers in dispersed systems. Communications systems based on Ethernet components similar to those found in PC networking systems suffered substantial degradation and damage effects when illuminated by the simulated albeit low-level EMP pulse. These damage effects are significant since they require the systems to be physically repaired or replaced in order to restore the normal communications capabilities.

Many of the effects noted in the previous paragraphs are attributed to the coupling to the wires and cables interconnecting the systems. The level of this coupling scales roughly with the length of the wire. As a general rule, the larger the transients are in the coupling lines, the more damaging they are to electronics equipment. It is therefore important to consider the transients that might be induced if a more distributed system encounters the same EMP electromagnetic energy. One way to address this concern is to perform cable coupling analysis. This was done as part of the current injection test program in order to relate the susceptibility levels of electronic equipment to the EMP threat.

At the system level, 100 percent of the control systems were affected at times. This is highly relevant to the prospect of system collapse and scope of the problem of restoration. This is more difficult to quantify at the subsystem level due to the sheer number of subsystems associated with each system. Translation to real world conditions must be tempered in cases where the control systems are located in structures that provide electromagnetic shielding of the incident EMP energy, but few of these exist in practice.

### ***Current Injection Testing***

Current injection testing was typically done by introducing transient voltage waveforms on a cable leading to the equipment under test. Depending on its load and that of the test generator, current was delivered to the test object. All of the electronics found in the power system is developed using a national (ANSI/IEEE) or international (IEC) standard

---

for a series of electromagnetic compatibility (EMC) waveforms that are representative of the transients observed during normal operation. One waveform that is commonly tested is known as the electrical fast transient (EFT). It has a rise time of 5 ns and a pulse width of 50 ns. By coincidence, this is very similar to the type of waveform coupled to cables by E1.

The objective of this testing was to determine at what level each type of equipment fails to operate normally and also to determine when operator intervention is necessary for the equipment to operate normally. Most of the equipment tested had multiple cable connections, covering different functions (power, signal, communications, etc.). These were all tested.

Given the levels of voltage in which the equipment malfunctioned, a separate effort was performed to compute the coupling of the incident E1 to cables with various lengths and orientations. For the long, exposed cables found in transmission substations, it was found that the induced voltage could exceed 20 kV under many circumstances.

In addition to free-field testing, the Commission sponsored a current injection testing program. The test program was representative in the sense that exemplars of most functional components were tested. Due to expense and time constraints, typically only one or two vendors' equipment was tested, and only one or two samples of a type were tested. The types of equipment tested and results brief are described in the following paragraphs:

***Electro-mechanical relays.*** These are the old-fashioned devices that contain no integrated circuits but function using high-power relays. They are still used in about 50 percent of applications, but that share is continuing to decline. As expected, these are immune to EMP upset up to the highest levels tested.

***Distribution line insulators.*** Earlier studies have indicated low vulnerability for these simple devices. The Commission-sponsored tests on a variety of 15kV class pin and suspension insulators indicate that there is a higher vulnerability than previously thought. New tests performed with the power on found that some insulators were destroyed due to the current following the path of the E1-induced arc. Statistical testing was not performed, so it is not clear what percentage of insulators will behave in this fashion; however, it is clear that power-on testing should be performed in the future to better understand this effect.

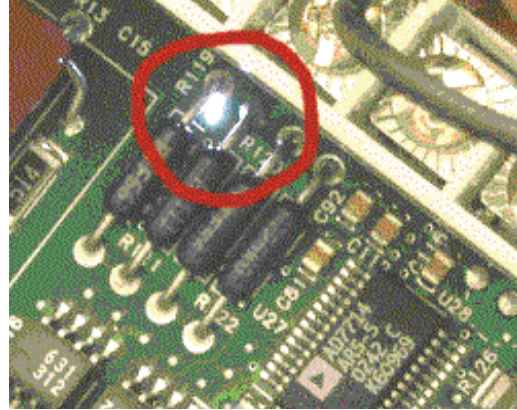
***Electronic protective relays.*** These devices (see **figure 2-5**) are the essential elements preserving high-value transmission equipment from damage during geomagnetic storms and other modes of grid collapse. Fortunately, these test items were the most robust of any of the electronic devices tested. However, test agencies reported that they are subject to upset at higher levels of simulated EMP exposure. We believe that altering the deployment configurations can further ameliorate the residual problems.



**Figure 2-5. Test Item: Electronic Relay**



*Programmable logic controllers and digital control systems.* These units are most commonly found in industrial settings and in particular are extensively used in power plants. They are subject to upset and damage at moderate levels of EMP assault (see **figure 2-6**). The circuit board pictured is from a typical PLC unit and is exhibiting a damaging short-circuit flashover during EMP Commission-sponsored testing.



**Figure 2-6. Flashover Observed During Injection Pulse Testing**

*General-purpose desktop computers and SCADA remote and master terminal units.* These were the most susceptible to damage or upset of all the test articles. Unlike the other kinds of devices tested, several different models and vintages were examined. The RS-232 ports were found to be particularly susceptible, even at very low levels of EMP stress.

With the exception of the RS-232 connections, all of the electronic devices that were tested performed up to the manufacturer's claimed levels for electromagnetic compatibility. Thus, the international standards to which the manufacturers subscribe are being met. Unfortunately the induced E1 stress is higher than the standards for normal operation.

The net result of this testing provides evidence that the power grid is also vulnerable to collapse due to the E1 component of an EMP assault, primarily through the upset and damage of the soft computer systems that are in common use. This however suggests that operational performance can be considerably enhanced at modest cost by attending to installation and configuration issues.

### Historical Insights

To provide insight into the potential impact of EMP-induced electronic system malfunctions, the Commission evaluated previous large service failure events. In these cases, similar (and less severe) system malfunctions have produced consequences in situations that were far too complex to predict using a model or analysis.

Another important observation is that these situations are seldom the result of a single factor but rather a combination of unexpected events, which are easily related to the impact only in hindsight. This is not surprising given the complexity, interdependency, and size of the systems involved. It is important to note that historical examples, while necessary for the insight they provide into the dependence of a functioning modern infrastructure on its automated control systems, do not remotely capture the scale of the expected EMP scenario. In an EMP event, it is not one or a few SCADA systems that are malfunctioning (the typical historical scenario) but very large numbers, hundreds or even thousands over a huge geographic area with a significant fraction of those rendered permanently inoperable until replaced or physically repaired. Critically, the systems that would identify what components are damaged and where they are located are also unavailable in many instances.

*Hurricane Katrina, August 2005.* Hurricane Katrina, one of the worst U.S. natural disasters ever, caused a widespread, multi-state blackout that lasted for a prolonged period, with catastrophic consequences for the afflicted region. The Katrina blackout was



a major factor in the failure of police, emergency and rescue services during the hurricane, which killed 1,464 people. The blackout caused gas stations to cease operating, paralyzing transportation and greatly impeding evacuation efforts. The Katrina blackout, which afflicted the region for weeks and lasted for months in some localities, so severely impeded recovery efforts that even today, 3 years later, New Orleans and its vicinity is still far from being fully recovered.

*August 14, 2003, Blackout.* The August 14 blackout was precipitated by a single line failure in one control area. It eventually affected nine control areas over a period of several hours, with rapidly spreading cascades of outage over the last 30 minutes. The extent of the blackout was exacerbated by deficiencies in specific practices, equipment, and human decisions. Initial retrospectives have focused on three likely contributory causes:

- ◆ Inadequate situational awareness at First Energy Corporation (FEC)
- ◆ FEC's failure to adequately manage tree growth in its transmission rights-of-way
- ◆ Failure of the interconnected grid's reliability organizations to provide effective diagnostic support.

The inadequate situational awareness and failure to provide effective diagnostic support are closely aligned to the computer and network effects that showed damage and upset during EMP testing. Additionally, new causal features (not common to other blackout incidents) of the August 14 blackout include inadequate interregional visibility over the power system, dysfunction of a control area's SCADA system, and lack of adequate backup capability to that system. Thus, all of the factors involved in the August 14 blackout are expected to be present in control areas impacted by an EMP event, but to a far greater extent. Therefore, an event as large as the ultimate August 14 blackout could be part of an initial EMP impact but multiplied several times over a contiguous geographical and system area. If this effect overlapped the Eastern and Western Interconnections, there is the increased probability that both interconnections could collapse.

*Western States Blackout.* The 1996 Western States blackout occurred when an electrically loaded transmission line sagged onto a tree and caused a short. This type of event is not uncommon, especially in the heavily treed areas of the Western Interconnect. At about the same time, a second line tripped (opened) due to improper protective relay activation. The tripping of the two transmission lines, coupled with a heavy electrical load on these lines and the thin margins on the transmission system, triggered the widespread outage through cascading failure. An EMP event could be expected to result in the loss of numerous transmission lines at once, not just the two cited in this case.

*Geomagnetic Storms.* Probably one of the most famous and severe effects from solar storms occurred on March 13, 1989. On this day, several major impacts occurred to the power grids in North America and the United Kingdom. This included the complete blackout of the Hydro-Quebec power system and damage to two 400/275 kV autotransformers in southern England. In addition, at the Salem nuclear power plant in New Jersey, a 1200 MVA, 500 kV transformer was damaged beyond repair when portions of its structure failed due to thermal stress. The failure was caused by stray magnetic flux impinging on the transformer core. Fortunately, a replacement transformer was readily available; otherwise the plant would have been down for a year, which is the normal delivery time for larger power transformers. The two autotransformers in southern England were also damaged from stray flux that produced hot spots, which caused significant gassing from the breakdown of the insulating oil.

The blackout of the Hydro-Quebec system was caused when seven static voltage-amps reactive (VAR) compensators (SVC) tripped and shut down due to increased levels of harmonics on the power lines. The loss of the seven SVCs led to voltage depression and frequency increase on the system, which caused part of the Quebec grid to collapse. Soon afterwards, the rest of the grid collapsed because of the abrupt loss of load and generation. The blackout took less than 90 seconds to occur after the first SVC tripped. About 6 million people were left without power for several hours and, even 9 hours later, there were still 1 million people without power.

Geomagnetic storms represent an approximation to an E3-induced voltage effect. The experience to date is of events that may be orders of magnitude smaller in scope and less severe than that expected from an EMP — although the Commission has also investigated the impact of a 100-year superstorm. The induced geomagnetic superstorm currents in the transmission lines will cause hundreds of high voltage transformers to saturate, creating a severe reactive load in the power system leading to voltage collapse in the affected area and damage to elements of the transmission system. The nature of this threat did not allow for experimental testing of the E3 effect, so this historical record is the best information on the effect.

### **Distinctions**

Past electric power blackouts provide a baseline for assessing the impact of an EMP attack on the power grid as discussed previously. However, there are several important factors that distinguish the EMP collapse scenario from these historical experiences.

- ◆ In the historical power system outages, only one or a few critical elements within an entire system have been debilitated. For example, a power generation facility may trip because a surge of current is unexpectedly presented through a fault from a particular load. Yet a substantial portion of the system may well be rendered out of service as the disruption triggers a series of cascading failures, each instigating the next failure (e.g., first a generator trips, then the frequency sags, and a load trips off or a transmission line trips out with its associated loads, which in turn causes the frequency to overrun and another generator trips out, and it continues to oscillate until the interconnected system comes down.) In the case of an EMP attack, elements within many critical facility components are likely to be damaged or disrupted simultaneously over a relatively broad geographic area, thus creating an almost certain cascading collapse of the remaining elements. Similarly, while lightning might strike a single plant, transmission line, or large load causing it to trip out, lightning has not hit multiple locations spread over a very wide area of the system with sufficient intensity and hitting all simultaneously to the extent that would be representative of an EMP attack.
  - ◆ During historical outages, the telecommunications system and associated control systems have continued to function. This provides the system operators with eyes and ears to know what was damaged, where damage occurred and in some cases the range of damage. While the power system may still come down, it is more possible to take protective measures to minimize damage and impact in order to effectuate rapid restoration. The communications and control systems' functionality are at high risk of disruption and damage themselves during an EMP attack. A minimum communications capability is needed to support immediate responses, to isolate parts for continued operation, and to implement necessary measures to restore the electrical system.
  - ◆ In the early stages of the EMP attack, even before the disruptions could be sensed and trips could occur that would lead to collapse, some or many of the protective devices
-

will be damaged that have ensured critical system components are safe to allow fast recovery. As a result, some and perhaps much of the electrical system would not be able to protect itself from the effects of multiple simultaneous and cascading failures. Widespread damage to the generation, transmission, and distribution infrastructures and equipment are probable. Rather than simply restoring power to an intact infrastructure with only a very few damaged components, the recovery task would be to replace an extensively damaged system under very difficult and decaying circumstances and then proceeding to restoration.

- ◆ The control systems would be damaged to some extent as opposed to remaining fully operational as in historical outages. The operations and dispatch centers where the vast interconnected system is controlled and managed would probably have damaged and disrupted components, the readings from the system would be fragmented and in many cases false or nonexistent, and communication by whatever means would be difficult to impractical to impossible. Control and knowledge would range from unreliable at best to simply nonexistent. Finding what and where damage has occurred and getting it repaired would be very problematic in any reasonable time frame, even within the control centers themselves, let alone out over the vast network with millions of devices.
- ◆ Skilled labor for a massive and diverse repair effort is not currently available if allocated over a large geographic area with great numbers of components and devices to check and repair where necessary. This scope of damage could cover perhaps 70 percent or possibly more of the continental United States as well as a significant part of Canada's population. This is far too large to bring in the limited skilled labor from very distant points outside the affected area in any reasonable time, even if one could coordinate them and knew where to send them, and they had the means to get there. Thus the extensive support from nearby fringe areas used so effectively in historical outages is likely to be unavailable as a practical matter as they themselves would be affected. The blackout resulting from Hurricane Katrina, an event comparable to a small EMP attack, overtaxed the ability of the Nation to quickly restore electric power, a failure that contributed to the slow recovery of the afflicted region.
- ◆ Other infrastructures would be similarly impacted simultaneously with the electrical system such as transportation, communication, and even water and food to sustain crews. The ability to find and get spare parts and components or purchase services would be severely hampered by lack of normal financial systems in addition to communication, transportation, and other factors. The Hurricane Katrina blackout caused precisely such problems.
- ◆ Fuel supplies for the power generation would be interrupted. First, the SCADA and DCS systems used in delivery of the fuel would be adversely impacted. In addition, much of the fuel supply infrastructure is dependent upon the electrical system. For example, natural gas-fired plants (which make up such a large share of the domestic generation) would be rendered inoperable since their fuel is delivered just in time for use. Coal plants have stockpiles that variously might be adequate for a week to a month. The few remaining oil-fired plants similarly have a limited storage of fuel. Nuclear plants would reasonably be expected to still have fuel but they would have to forego protective regulations to continue to operate. Many renewable fueled resources would still have their fuel supply but EMP effects on controls may still render them inoperable.

It is not possible to precisely predict the time to restore even minimal electrical service due to an EMP eventuality given the number of unknowns and the vast size and complexity of the system with its consequent fragility and resiliency. Expert judgment and rational extrapolation of models and predictive tools suggest that restoration to even a diminished but workable state of electrical service could well take many weeks, with some probability of it taking months and perhaps more than a year at some or many locations; at that point, society as we know it couldn't exist within large regions of the Nation. The larger the affected area and the stronger the field strength from the attack (corollary to extent of damage or disruption), the longer will be the time to recover. Restoration to current standards of electric power cost and reliability would almost certainly take years with severe impact on the economy and all that it entails.

### **Strategy**

The electrical system must be protected against the consequences of an EMP event to the extent reasonably possible. The level of vulnerability and extreme consequence combine to invite an EMP attack. Thus reduction of our vulnerability to attack and the resulting consequences reduces the probability of attack. It is also clear the Cold War type of deterrence through mutual assured destruction is not an effective threat against many of the potential protagonists, particularly those who are not identifiable nation-states. The resulting strategy is to reduce sharply the risk of adverse consequences from an EMP attack on the electrical system as rapidly as possible. The two key elements of the mitigation strategy for the electrical system are protection and restoration.

The initial focus for reducing adverse consequences should be on the restoration of overall electrical system performance to meet critical, if not general, societal needs. The focus should be on the system as a whole and not on individual components of the system. Timely restoration depends on protection, first of high-value assets, protection necessary for the ability to restore service quickly to strategically important loads, and finally protection as required to restore electrical service to all loads. The approach is to utilize a comprehensive, strategic approach to achieve an acceptable risk-weighted protection in terms of performance, schedule, timing, and cost. The effort will include evolution to greater and greater levels of protection in an orderly and cost-effective manner consistent with the anticipated threat level. Where possible, the protection also will enhance normal system reliability and, in so doing, provide great service to society overall.

There is a point in time at which the shortage or exhaustion of critical items like emergency power supply, batteries, standby fuel supplies, replacement parts, and manpower resources which can be coordinated and dispatched, together with the degradation of all other infrastructures and their systemic impact, all lead toward a collapse of restoration capability. Society will transition into a situation where restoration needs increase with time as resources degrade and disappear. This is the most serious of all consequences and thus the ability to restore is paramount.

### **Protection**

It is not practical to try to protect the entire electrical power system or even all high-value components from damage by an EMP event. There are too many components of too many different types, manufactures, ages, and designs. The cost and time would be prohibitive. Widespread collapse of the electrical power system in the area affected by EMP is virtually inevitable after a broad geographic EMP attack, with even a modest number

of unprotected components. Since this is a given, the focus of protection is to retain and restore service to critical loads while permitting relatively rapid restoration.

The approach to protection has the following fundamental aspects. These will collectively reduce the recovery and restoration times and minimize the net impact from assault. All of this is feasible in terms of cost and timing if done as part of a comprehensive and reasonable response to the threats, whether the assault is physical, electromagnetic (such as EMP), or cyber.

1. Protect high-value assets through hardening. Hardening, providing for special grounding, and other schemes are required to assure the functional operation of protection equipment for large high-value assets such as transformers, breakers, and generators and to so protect against sequential, subsequent impacts from E2 and E3 creating damage. Protection through hardening critical elements of the natural gas transportation and gas supply systems to key power plants that will be necessary for electrical system recovery is imperative.
  2. Assure there are adequate communication assets dedicated or available to the electrical system operators so that damage during system collapse can be minimized; components requiring human intervention to bring them on-line are identified and located; critical manpower can be contacted and dispatched; fuel, spare parts and other commodities critical to the electrical system restoration can be allocated; and provide the ability to match generation to load and bring the system back on line.
  3. Protect the use of emergency power supplies and fuel delivery, and importantly, provide for their sustained use as part of the protection of critical loads, which loads must be identified by government but can also be assured by private action. Specifically:
    - Increase the battery and on-site generating capability for key substation and control facilities to extend the critical period allowing recovery. This is relatively low cost and will improve reliability as well as provide substantial protection against all forms of attack.
    - Require key gasoline and diesel service stations and distribution facilities in geographic areas to have at-site generation, fueled off existing tanks, to assure fuel for transportation and other services, including refueling emergency generators in the immediate area.
    - Require key fueling stations for the railroads to have standby generation, similar to that required for service stations and distribution facilities.
    - Require the emergency generator start, operation, and interconnection mechanisms to be EMP hardened or manual. This will also require the ability to isolate these facilities from the main electrical power system during emergency generation operation and such isolation switching must be EMP hardened.
    - Make the interconnection of diesel electric railroad engines and large ships possible and harden such capability, including the continued operation of the units.
    - The Government must determine and specify immediately those strategically important electrical loads critical to the Nation to preserve in such an emergency.
  4. Separate the present interconnected systems, particularly the Eastern Interconnection, into several nonsynchronous connected subregions or electrical islands. It is very important to protect the ability of the system to retain as much in operation as possible through reconfiguration particularly of the Eastern Connected System into a number of nonsynchronous connected regions, so disruptions will not cascade beyond those EMP-disrupted areas. Basically, this means eliminating total NERC region service loss, while at the same time maintaining the present interconnection status with
-



its inherent reliability and commercial elements. This is the most practical and easiest way to allow the system to break into islands of service and greatly enhance restoration timing. This will not protect most within the EMP-insult area, but it should increase the amount of viable fringe areas remaining in operation. This is fiscally efficient and can leverage efforts to improve reliability and enhance security against the broader range of threats, not only EMP. It also can be beneficial to normal system reliability.

5. Install substantially more black start generation units coupled with specific transmission that can be readily isolated to balancing loads. The NERC regions now do surveys of available black start and fuel switchable generation. Requiring all power plants above a certain significant size to have black start or fuel-switching capability (with site-stored fuel) would be a very small added expense that would provide major benefits against all disruptions including nonadversarial ones. Black start generator, operation, and interconnection mechanisms must be EMP hardened or be manual without microelectronic dependence. This also will require the ability to isolate these facilities from the main electrical power system during emergency generation operation and that isolation switching is EMP hardened. In addition, sufficient fuel must be provided, as necessary, to substantially expand the critical period for recovery.
6. Improve, extend, and exercise recovery capabilities. Develop procedures for addressing the impact of such attacks to identify weaknesses, provide training for personnel and develop EMP response training procedures and coordinate all activities and appropriate agencies and industry. While developing response plans, training and coordination are the primary purpose.

### ***Recovery and Restoration***

The key to minimizing catastrophic impacts from loss of electrical power is rapid restoration. The protective strategy described is aimed primarily at preserving the system in a recoverable state after the attack, maintaining service to critical loads, and enhancing recovery.

The first step in recovery is identifying the extent and nature of the damage to the system and then implementing a comprehensive plan with trained personnel and a reservoir of spare parts to repair the damage. Damage is defined as anything that requires a trained person to take an action with a component, which can include simply rebooting all the way to replacing major internal elements of the entire component. A priority schedule for repair of generation, transmission, and even distribution is necessary since resources of all types will be precious and in short supply should the EMP impact be broad enough and interdependent infrastructures be adversely impacted (e.g., communication, transportation, financial and life-supporting functions).

Restoration is complicated in the best of circumstances, as experienced in past black-outs. In the instance of EMP attack, the complications are magnified by the unprecedented scope of the damage both in nature and geographical extent, by the lack of information post attack, and by the concurrent and interrelated impact on other infrastructures impeding restoration.

Restoration plans for priority loads are a key focus. Widely scattered or single or small group loads are in most cases impractical to isolate and restore individually given the nature of the electrical system. These are to be served first through the emergency power supply aspects identified in the Protection section. Restoration of special islands can,



however, be made practical by the nonsynchronous connected subregions if they are identified by the Government as necessary very far in advance of any assault. Otherwise, the system's resources and available personnel will need to act expeditiously to get as many islands of balanced load and generation back into operation. This will begin by system operators identifying those easiest to repair (normally the least damaged) and restore them first. As these stabilize, the system recovery will flow outward as, increment by increment, the system is repaired and brought back in service. It is much more feasible and practical to restore by adding incrementally to an operating island rather than black starting the recovery for an island.

Balancing an isolated portion of generation and load first, and then integrating each new increment is a reasonably difficult and time-consuming process in the best of circumstances. In an EMP attack with multiple damaged components, related infrastructure failures, and difficulty in communications, restoring the system could take a very long time unless preparatory action is taken.

Generating plants have several advantages over the widely spread transmission network as it relates to protection and restoration from an EMP event. The plant is one complete unit with a single DCS control network. It is manned in most cases so operators and maintenance personnel are immediately available and on site. The operating environment electronically requires a level of protection that may provide at least a minimal protection against EMP. Nevertheless, it is important to harden critical controls sufficiently to enable manual operation at a minimum. Providing for at-site spares to include the probably needed replacements for control of operation and safety would be straightforward and not expensive to accomplish, thus assisting rapid restoration of capability.

As controls and other critical components of the electrical transmission and generation system suffer damage, so do similar components on the production, processing, and delivery systems providing fuel to the electric generators. Restoration of the electrical power system is not feasible on a wide scale without a parallel restoration of these fuel processing and delivery systems.

Hydropower, wind, geothermal, and solar power each has a naturally reoccurring fuel supply that is unaffected by EMP. However, the controls of these plants themselves are subject to damage by EMP at present. In addition, only hydropower and geothermal have controllable fuel (i.e. they can operate when needed versus wind and solar that operate when nature provides the fuel just-in-time). As a practical matter, only hydropower is of sufficient size and controllability in some regions to be a highly effective resource for restoration, such as the Pacific Northwest, the Ohio/Tennessee valley, and northern California. Beyond the renewable resources, coal and wood waste plants typically have significant stockpiles of fuel so the delay in rail and other delivery systems for a couple of weeks and in some instances up to a month is not an issue for fuel. Beyond that, rail and truck fuel will be needed and delivery times are often relatively slow, so the delivery process must start well before the fuel at the generator runs out.

Operating nuclear plants do not have a fuel problem per se, but they are prohibited by regulation from operating in an environment where multiple reliable power supply sources are not available for safe shutdown, which would not be available in this circumstance. However, it is physically feasible and safe for nuclear plants to operate in such a circumstance since they all have emergency generation at site. It would simply have to be fueled sufficiently to be in operation when the nuclear plant is operating without external

---

electrical supply sources. Nuclear power backup would need to be significantly expanded. Natural gas-fired power plants are very important in restoration because of their inherent flexibility and often their relatively small size, yet they have no on-site fuel storage and are totally dependent upon the natural gas supply and gas transportation system which are just in time for this purpose. Therefore, the natural gas fuel delivery system must be brought back on-line before these power plants can feasibly operate. It is operated largely with gas turbines of its own along the major pipelines. The key will be to have the protection, safety, and controls be hardened against EMP.

Recovery from transmission system damage and power plant damage will be impeded primarily by the manufacture and delivery of long lead-time components. Delivery time for a single, large transformer today is typically one to two years and some very large special transformers, critical to the system, are even longer. There are roughly 2,000 transformers in use in the transmission system today at 345 kV and above with many more at lesser voltages that are only slightly less critical. No transformers above 100 kV are produced in the United States any longer. The current U.S. replacement rate for the 345 kV and higher voltage units is 10 per year; worldwide production capacity of these units is less than 100 per year. Spare transformers are available in some areas and systems, but because of the unique requirements of each transformer, there are no standard spares. The spares also are owned by individual utilities and not generally available to others due to the risk over the long lead time if they are being used. Transformers that will cover several options are very expensive and are both large and hard to move. NERC keeps a record of all spare transformers.

Recovery will be limited by the rate of testing and repair of SCADA, DCS, and PLC and protective relay systems. With a large, contiguous area affected, the availability of outside assistance, skilled manpower, and spares may well be negligible in light of the scope of the problem. Information from power industry representatives enables us to place some limits on how long the testing and repair might take. Determining the source of a bad electrical signal or tiny component that is not working can take a long time. On the low side, on-site relay technicians typically take three weeks for initial shakedown of a new substation. Simply replacing whole units is much faster, but here too, inserting new electronic devices and ensuring the whole system works properly is still time consuming. It must be noted that the substations are typically not manned so skilled technicians must be located, dispatched, and reach the site where they are needed. Many of these locations are not close to the technicians. It is not possible to readily estimate the time it will take in the event of an EMP attack since the aftermath of an EMP attack would not be routine and a certain level of risk would likely be accepted to accelerate return to service. It seems reasonable, then, to estimate an entire substation control system recovery time to be at least several days, if not weeks. This assumes that the trained personnel can reach the damaged locations and will be supported with water, food, communication, spare parts, and the needed electronic diagnostic equipment.

Unlike generation, recovery of the transmission system will require off-site communications because coordination between remote locations is necessary. Communications assets used for this purpose now include dedicated microwave systems and, increasingly, cell phones and satellite systems. If faced with a prolonged outage of the telecommunications infrastructures, repairs to dedicated communication systems or establishment of new ad-hoc communications will be necessary. This might take one or more weeks and

would set a lower limit on recovery time, but it would be unlikely to affect the duration of a months-long outage.

Restoration to electrical service of a widely damaged power system is complex. Beginning with a total blackout, it requires adequate communication to match and coordinate a generating plant to a load with an interconnected transmission that normally can be isolated via switching at several substations, so it is not affected by other loads or generation. The simultaneous loss of communication and power system controls and the resulting lack of knowledge about the location of the damage all greatly complicate restoration. There are also a diminishing number of operators who can execute the processes necessary for restoration without the aid of computers and system controls.

Without communication, both voice and data links, it is nearly impossible to ascertain the nature and location of damage to be repaired, to dispatch manpower and parts, and to match generation to load. Transportation limitations further impede movement of material and people. Disruption of the financial system will make acquisition of services and parts difficult. In summary, actions are needed to assure that difficult and complex recovery operations can take place and be effective in an extraordinarily problematic post-attack environment.

The recovery times for various elements of the electrical system are estimated in the following paragraphs. These should be regarded as very rough best estimates for average cases derived from the considered judgment of several experts. These estimates are gross averages, and the situation would vary greatly from one facility to another as the situation, number of disrupted and damaged elements and the extent of preassault preparedness and training vary. In addition, the contingencies and backlogs strongly depend on the extent of such damage elsewhere and are essentially unknown. For example, fuel delivery capability is a key element. Each of the system elements — generation (including fuel delivery), transmission, distribution, and often load — must be repaired and in working order sufficient for manual control at a minimum (each element with skilled personnel all in communication with each other). Thus, the following should be occurring in parallel as much as possible, but in some instances testing of one element requires a working capability of another. The availability of spare parts and trained manpower coupled with knowledge of what to repair and where it is are critical to recovery timing. The recovery times provided below are predicated upon the assumption that the other infrastructures are operating normally. The recovery times would increase sharply with the absence of other operating infrastructures, which is likely in the EMP situation. These estimates are based upon present conditions, not what is possible if the Commission recommendations are followed.

#### *Power Plants*

- ◆ Replace damaged furnace, boiler, turbine, or generator: one year plus production backlog plus transportation backlog. It is uncertain if and to what extent damage to these elements will occur if the protection schemes are disrupted or damaged.
- ◆ Repair some equipment if spares on site exist, but repair time depends on the type of plant and personnel available at the plant at the time of the assault: two days to two weeks plus service backlog at the site or to move trained personnel from plant to plant.
- ◆ Repair and test damaged SCADA, DCS, and computer control system: three months.
- ◆ Return repaired or undamaged plant to operation, provided the major components under the first bullet are not damaged: (1) nuclear: three days provided there is an

independent power feed with enough fuel, which should be on site in such an emergency, (2) coal: two days plus black start or independent power feed, (3) natural gas: two hours to two days depending on fuel supply and black start, (4) hydro: immediate to one day, (5) geothermal: one to two days, (6) wind: immediate to one day unless each turbine requires inspection and then one or two turbines a day.

- ◆ All of the above are also contingent on the availability of fuel. Our recommendations for on-site reserves: coal: 10-30 days; natural gas: depends on whether the pipeline is operating; nuclear: 5 days to several weeks; hydro: depends on reservoir capacity available for continued use.

#### *Transmission and Related Substations*

- ◆ Replace irreparably damaged large transformers: One to two years plus production backlog plus transportation plus transportation backlog (these are very large and require special equipment to transport that may not be available in this situation).
- ◆ Repair damaged large transformer: one month plus service backlog.
- ◆ Repair manual control system: one month if adequate personnel are available.
- ◆ Establish ad hoc communications: one day to two weeks.
- ◆ Repair and test damaged protective systems: three months.
- ◆ Repair and return of substations to service are also contingent on the local availability of power. All substations have batteries for uninterrupted power, nominally enough for eight hours. Very few (about 5 percent) have on-site emergency generators. Many utilities rented emergency generators in advance of the Y2K transition. Almost all are now gone. Once the local power is gone, other emergency power often must be brought to the station for operation.
- ◆ Assuming DC terminals are manned: one week to one month depending upon damage.

#### *Distribution and Related Substations*

- ◆ Replace insulators that have flash-over damage: two to five days, unless very widespread and then weeks.
- ◆ Replace service transformers: two to five days unless very widespread and then weeks.
- ◆ Repair time depends on the number of spares, available crews that perform the repairs, and equipment.
- ◆ Note that the load on the end of the distribution may have some disruption that needs repair as well.

Starting an electrical power system from a fully down and black system requires one of the following two approaches. (1) At the margin of the outage, an operating electrical system is running at proper frequency with balanced load to generation, and this system can be interconnected to the fringe of the black portion of the system. The newly interconnected portion, the portion being restored, must be able to sequentially (in increments or simultaneously) bring on load and generation to keep the now larger portion of the system in sufficient frequency balance so the entire system, new and old, does not collapse. Then another increment is integrated into the operating system and so on. As the portion that is operating in balance becomes larger and more flexible, the increments that are able to be added become larger as well, since the operating system can absorb more and maintain stability. This is how historical outage areas are predominantly restarted. (2) There is generation that can be black started. This means starting a generator without an external power source, such as hydroelectric or diesel generation. To do this, the genera-

tion has to be synchronized on line, and a load has to be matched to the generation as it comes on line. That requires that a transmission link between the generation and the load be put in service. Yet the transmission link also must be segregated from the rest of the system, or the load hanging on it would be too large. Both approaches require that the increment of the system being re-energized to be fully functional (repaired) and communication established between the generation and load, including any substation or switchyard between the two. Importantly, it requires skilled personnel to execute the restoration manually.

The generation must have sufficient fuel to accommodate the load being met in balance. Water behind a hydroelectric facility may be limited and certainly the diesel fuel is likely to be limited. Thus the startup must be done carefully because failures could render the black start inoperable as it runs out of fuel or depletes the battery. Normally, in this type of situation, the diesel or small hydro is used primarily to start up a larger generator of a size that can carry the necessary load increment. This larger generator must be fueled, which can be a complication as discussed elsewhere in this chapter.

Under deregulation, the disconnection (in the business sense) of transmission from generation that has been occurring in the U.S. electrical power business creates a problem for black start recovery. There are risks involved in returning a plant to operation and costs for the needed repairs. Questions about who will pay whom and who will follow whose direction is not easy to answer, even with everybody wanting to cooperate. Under the historic utility monopolies, the generation and the transmission assets had a common owner, so these matters were handled within a single organization. Now, coordination with independent power producers is nearly unenforceable other than through heavy government emergency powers noting that power producers and owners want indemnification before assuming risk. Therefore some degree of command authority is required for coordination, assessment, and acceptance of risk of damage and financial settlement of losses.

The time to integrate sufficient portions of a black region of the system using the fringe approach is reasonably short if the outage area is small in relation to the operating area as has been seen in past outage conditions. In the case of EMP, where the outage area is likely to be much larger than the fringe area or there is no fringe area, restoration of even parts will be measured in weeks to months. If communication is difficult to nonexistent, restoration can take much longer.

### ***Mitigation of Adverse Consequences***

By protecting key system components, structuring the network to maximize fringe service, through the nonsynchronous interconnections, expanding the black start and system emergency power support, creating comprehensive recovery plans for the most critical power needs, and providing adequate training of personnel, the risk of catastrophic impact to the Nation can be significantly reduced. The mitigation plan must be jointly developed by the Federal Government and the electric power industry, instilled into systems operations, and practiced to maintain a ready capability to respond. It must also be fully coordinated with the interdependent infrastructures, owners, and producers.

The continuing need to improve and expand the electric power system as a normal course of business provides an opportunity to judiciously improve both security and reliability in an economically acceptable manner — provided that technically well-informed decisions are made with accepted priorities. There are a wide variety of potential threats



besides EMP that must be addressed, which can have serious to potentially catastrophic impacts on the electrical system. Common solutions must be found that resolve these multiple vulnerabilities as much as possible. For example, in the course of its work, the Commission analyzed the impact of a 100-year solar storm (similar to E3 from EMP) and discovered a very high consequence vulnerability of the power grid. Steps taken to mitigate the E3 threat also would simultaneously mitigate this threat from the natural environment. Most of the precautions identified to protect and restore the system from EMP will also apply to cyber and physical attacks. The Commission notes that the solutions must not seriously penalize our existing and excellent system but should enhance its performance wherever possible.

The time for action is now. Threat capabilities are growing and infrastructure reinvestment is increasingly needed which creates an opportunity for the investment to serve more than one purpose. Government must take responsibility for improvements in security. As a general matter, improvements in system security are a Government responsibility, but it may also enhance reliability if done in certain ways. For example, providing spare parts, more black start capability, greater emergency back-up, nonsynchronous interconnections, and more training all will do so. Yet, EMP hardening components will not increase reliability or enhance operation. Conversely improving reliability does not necessarily improve security, but it may if done properly. For example, adding more electronic controls will not enhance EMP security, but electronic spare parts and more skilled technicians will help improve security and reliability. Finding the right balance between the utility or independent power producer's service and fiscal responsibility with the Government's security obligation as soon as possible is essential, and that balance must be periodically (almost continuously) reexamined as technology and system architecture changes.

## **Recommendations**

EMP attack on the electrical power system is an extraordinarily serious problem but one that can be reduced below the level of a catastrophic national consequence through focused effort coordinated between industry and government. Industry is responsible for assuring system reliability, efficiency, and cost effectiveness as a matter of meeting required service levels to be paid for by its customers. Government is responsible for protecting the society and its infrastructure, including the electric power system. Only government can deal with barriers to attack — interdiction before consequence. Only government can set the standards necessary to provide the appropriate level of protection against catastrophic damage from EMP for the civilian sector. Government must validate related enhancements to systems, fund security-only related elements, and assist in funding others.

It must be noted, however, that the areas where reliability and security interact represent the vast majority of cases. The power system is a complex amalgamation of many individual entities (public, regulated investor-owned, and private), regulatory structures, equipment designs, types and ages (with some parts well over one hundred years old and others brand new). Therefore, the structure and approach to modifications must not only recognize the sharply increased threat from EMP and other forms of attack, but improvements must be accomplished within existing structures. For example, industry investment to increase transmission capacity will improve both reliability and system security during the period when transmission system operating margins are increased.

The Commission concluded that mitigation for a majority of the adverse impact to the electrical system from EMP is reasonable to undertake in terms of time and resources. The specific recommendations that follow have been reviewed with numerous entities with responsibility in this area. The review has been in conceptual terms, with many of the initiatives coming from these parties, but the recommendations are the Commission's responsibility alone. The activities related to mitigation of adverse impacts on fuel supply to electric generation are more fully discussed in a separate chapter of this report.

### ***Responsibility***

As a result of the formation of Department of Homeland Security (DHS) with its statutory charter for civilian matters, coupled with the nature of EMP derived from adversary activity, the Federal Government, acting through the Secretary of Homeland Security, has the responsibility and authority to assure the continuation of civilian U.S. society as it may be threatened through an EMP assault and other types of broad scale seriously damaging assaults on the electric power infrastructure and related systems.

It is vital that DHS, as early as practicable, make clear its authority and responsibility to respond to an EMP attack and delineate the responsibilities and functioning interfaces with all other governmental institutions with individual jurisdictions over the broad and diverse electric power system. This is necessary for private industry and individuals to act to carry out the necessary protections assigned to them and to sort out liability and funding responsibility. DHS particularly needs to interact with FERC, NERC, state regulatory bodies, other governmental institutions at all levels, and industry in defining liability and funding relative to private and government facilities, such as independent power plants, to contribute their capability in a time of national need, yet not interfere with market creation and operation to the maximum extent practical.

DHS, in carrying out its mission, must establish the methods and systems that allow it to know, on a continuous basis, the state of the infrastructure, its topology, and key elements. Testing standards and measurable improvement metrics should be defined as early as possible and kept up to date.

The NERC and the Electric Power Research Institute (EPRI) are readily situated to provide much of what is needed to support DHS in carrying out its responsibilities. The Edison Electric Institute, the American Public Power Association, and the North American Rural Electric Cooperative Association are also important components for coordinating activity. Independent power producers and other industry groups normally participate in these groups or have groups of their own. The manufacturers of generation, transmission, and distribution components are another key element of the industry that should be involved. Working closely with industry and these institutions, DHS should provide for the necessary capability to control the system in order to minimize self-destruction in the event of an EMP attack and to recover as rapidly and effectively as possible.

### ***Multiple Benefit***

Most of the recommended initiatives and actions serve multiple purposes and thus are not only to mitigate or protect against an EMP attack and other assaults on the electric power system. The protection of the system and rapid restoration of the system from an EMP attack also are effective against attack from a number of physical threats that directly threaten to destroy or damage key components of the electrical system. Large-scale natural disasters, such as Hurricane Katrina, also are in large part mitigated by these

---

same initiatives. Many of the initiatives enhance reliability, efficiency, and quality of the electrical supply, which is a direct benefit to the electrical consumer and the U.S. economy.

To the greatest extent feasible, solutions for EMP should be designed to be useful solutions to the broad range of security and reliability challenges. For example, black start resources are essential for many threats, purposeful or not, to the power grid. Integrating cyber security and EMP hardness into control systems simultaneously as these systems are routinely upgraded will be much more effective and less costly than doing two separate jobs.

### ***Recommended Initiatives***

The following initiatives must be implemented and verified by DHS and DOE, utilizing industry and other governmental institutions to assure the most cost effective outcome occurs and that it does so more rapidly than otherwise possible. In many instances, these initiatives are extensions or expansions of existing procedures and systems such as those of NERC.

- ◆ *Understand system and network level vulnerabilities, including cascading effects*—To better understand EMP-related system response and recovery issues, conduct in-depth research and development on system vulnerabilities. The objective is to identify cost effective and necessary modifications and additions in order to further achieve the overall system performance. Specifically there should be government-sponsored research and development of components and processes to identify and develop new consequential and cost effective approaches and activities.
- ◆ *Evaluate and implement quick fixes*—Identify what may presently be available commercially to provide cost effective patches and snap-on modifications to quickly provide significant protection and limit damage to high-value generation and transmission assets as well as emergency generation and black start capability. These include installation or modification of equipment as well as changes in operating practices. This is both fast and low cost.
- ◆ *Develop national and regional restoration plans*—The plans must prioritize the rapid restoration of power with an emphasis on restoring critical loads that are identified by the Government. The plans must be combined with the requirements for providing and maintaining emergency power service by these loads. The plans must address outages with wide geographic effect, multiple component failure, poor communication capability, and failure of islanding schemes within the affected area. Government and industry responsibilities must be assigned and clearly delineated. Indemnification arrangements must be put into place to allow industry to implement the Government's priorities as well as deal with potential environmental and electrical hazards to ensure rapid recovery. Planning must address not only the usual contingency for return to normal operating condition, but also restoration to a reduced capability for minimum necessary service. Service priorities under duress may be different from priorities under normal conditions. The planning basis for reduced capability should be the minimum necessary connectivity, generation assumptions based on reduced fuel availability scenarios, and reduced load, with the goal of universal service at limited power. National Guard and other relevant resources and capabilities must be incorporated.
- ◆ *Assure availability of replacement equipment*—On hand or readily available spare parts to repair or replace damaged electronic and larger power system components

must be available in sufficient quantities and in locations to allow for rapid correction and restoration commensurate with a post-EMP attack and its impacts on related infrastructures such as communication and transportation. NERC already has a spare component database for such large items as transformers and breakers that is expanding to include delivery capability, but now must be revised to accommodate an EMP attack environment. Where additional spare components need to be acquired or delivery made possible to critical locations, DHS must work with NERC and industry to identify the need and provide the spares or delivery capability; such as the critical material and strategic petroleum reserves and similar strategic reserves. The key will be to decide where to draw the line between reserves for reliability and those for security. It also will be necessary to keep the equipment current. In addition, strategic manufacturing and repair facilities themselves might be provided with emergency generation to minimize stockpiles. This would also be of benefit to industry as well as enhance security. Research is underway and should be further pursued, into the production of multiple use emergency replacement transformers, breakers, controls, and other critical equipment. Such devices would trade efficiency and device service life for modularity, transportability and affordability. They would not be planned for normal use. Movement, stockpiles and protection of stockpiles must be integrated with National Guard and other relevant capabilities.

- ◆ *Assure availability of critical communications channels*—Assure that throughout the system there are local and system-wide backup EMP survivable communication systems adequate for command and control of operations and restoration of the electrical system. The most critical communications channels are the ones that enable recovery, not normal operations. Planning must presume that, for the near term at least, computer-based control systems will not be capable of supporting post-EMP operations. The most critical communication assets are thus the in-house ones that enable manual operation and system diagnostics. Dispatch communication is next in importance. Communications to coordinate black start are also vital. NERC should review and upgrade operating procedures and information exchanges between and among existing control centers, key substations, and generating plants to recognize and deal as effectively as possible with EMP, building upon the systems, procedures, and databases currently in place. Local emergency and 9-1-1 communications centers, the National Guard and other relevant communication systems, and redundant capabilities should be incorporated where possible.
- ◆ *Expand and extend emergency power supplies*—Add to the number of stand-alone back-up and emergency power supplies such as diesels and long-life batteries. This addition is vital and a least-cost protection of critical service. The loss of emergency power before restoration of the external power supply is likely to occur in present circumstances and is highly probable to be devastating. Presently such emergency power is useable only for relatively short periods due mostly to at-site stored fuel limitations, which have become increasingly limited. The length of time recommended for each location and load will be determined by DHS and industry where the emergency supply is private, such as with hospitals, financial institutions, and telecommunication stations. The specific recommendations are:
  - Increase the battery and on-site generating capability for key substation and control facilities to extend the critical period allowing recovery. This action is relatively low cost and will improve reliability as well as provide substantial protection against all forms of attack.

- Require key gasoline and diesel fuel service stations and liquid fuel distribution facilities in geographic areas to have at-site generation, fueled from existing at-site storage to assure fuel for transportation and other services, including refueling emergency generators in the immediate area.
  - Require that key fueling stations for the railroads have standby generation much as the previously mentioned service stations and distribution facilities.
  - Require the emergency generator start, operation, and interconnection mechanisms to be EMP hardened or manual. This action will also require the ability to isolate these facilities from the main electrical power system during emergency generation operation and require that such isolation switching be EMP hardened.
  - Where within safety parameters extend the emergency generation life through greater fuel storage or supply sources (with their own emergency power supplies). Fuel supplies for more critical facilities must be extended to at least a week or longer, where possible. This action will probably entail careful use or development of relatively near location (but not contiguous) fuel stockpiles with their own emergency generation.
  - Regularly test and verify the emergency operations. If the Government were to enforce current regulations, many of the public facilities with standby generation would be routinely tested and failures could be avoided.
  - Provide for the local integration of railroad mobile diesel electric units with switching and controls hardened against EMP. The same should be provided for large ships at major ports.
- ◆ *Extend black start capability*—Systemwide black start capabilities must be assured and exercised to allow for smaller and better islanding and faster restoration. The installation of substantially more black start generations units and dual feed capable units (e.g., natural gas-fired units that can operate on #2 oil stored on site) coupled with specific transmission that can be readily isolated to balance loads for restoration is necessary. Sufficient fuel must be provided to substantially expand the critical period for recovery such as with multiple start attempts. The NERC regions now do surveys of available black start and fuel switchable generation. Requiring all power plants above a certain significant size to have black start or at-site fuel switching capability (with at-site stored fuel) would be a very small added expense, and would provide major benefits against all disruptions including nonadversarial, so it is both an industry and security benefit. The start, operation, and control systems for such capability have to be EMP hardened or manual, recognizing that most large power plants have personnel on site.
- ◆ *Prioritize and protect critical nodes*— Government entities, such as DHS and DOE, must identify promptly those specific loads that are critical to either remain in service or to be restored as a priority with target restoration to be within a matter of hours following an EMP attack. These may well include loads necessary to assure the continuation of all forms of emergency response care and recovery. These must include what is necessary to avoid collapse of, or allow for the rapid recovery of financial systems, key telecommunication systems, the Government's command and control in the civilian sector, and those elements that allow for rapid and effective recovery of the electric power system in a more general sense. These loads must be prioritized so that the most critical can be protected and designed for rapid restoration in the near term and then add more next-level priority loads as resources permit. The above recommendations for extended and adequate emergency power supply are the most direct
-



and cost efficient approach. The shift to nonsynchronous, interconnected islands is the secondary application, but it will take longer and is more expensive. Providing such islands of small-to-modest size to support large loads can best assure no loss of power supply or far more rapid restoration.

- ◆ *Expand and assure intelligent islanding capability*—Direct the electrical system institutions and entities to expand the capability of the system to break into islands of matching load and generation, enhancing what now exists to minimize the impact and provide for more rapid and widespread recovery. The establishment of nonsynchronous connections between subregions, perhaps beginning with NERC already identified subregions, should be required. This can readily be accomplished today with approaches such as DC back-to-back converter installations that facilitate power transfers but maintain a barrier. This mode of operation between regions is often referred to as maintaining frequency independence. Reconfiguration of the Eastern Connected System into a number of such nonsynchronous connected regions could eliminate large service interruptions, while still maintaining the present interconnection status. It may be a priority to first establish smaller islands of frequency independence to better assure power supply to government-identified critical loads that are nominally too large for most emergency power supplies, such as large financial centers, and telecommunication hubs. Incidental to any studies could be new ideas for conversion of HVAC transmission lines to HVDC operation for greater transmission capacity as a further and corollary benefit. Also new ideas are being discussed, such as, where the converter transformers can be eliminated, resulting in a substantial cost reduction. Asynchronous regional connections is a common term used to identify this broad area technically. The protective and control systems necessary to implement this capability will have to be hardened. It will not be a retrofit but simply a part of the initial design and procedures, so the cost for EMP protection is small. Note that the DC or other interface making the nonsynchronous connection possible is not sized for the entire electrical capacity within the respective island but is sufficient only for reliability and commercial transactions, which normally is far less. Sizing this interface is a special effort that needs to be established primarily by NERC and FERC but with Federal coordination. Breaking the larger electrical power system into subsystem islands of matching load and generation will enhance what now exists to minimize the impact, decrease likelihood of broad systemwide collapse, and provide for more rapid and widespread recovery. It is just as useful for normal reliability against random disturbances or natural disasters in reducing size and time for blackouts. Thus it is critical for protection and restoration coming from any type of attack, not just EMP. Ensuring this islanding capability in the event of EMP is critical, although it requires a longer-term system design and implementation.

- ◆ *Assure protection of high-value generation assets*—Enhance the survivability of generating plants at the point of system collapse due to the very broad and simultaneous nature of an EMP attack. NERC, EPRI, equipment and control system providers, and utilities need to aggressively evaluate and verify what is vulnerable to EMP and commensurate consequences. Generating plants can be severely damaged from large electrical faults or incursions in the absence of protective devices. They can also be occasionally damaged in the event of sudden load loss if protective shutdown systems fail. Control systems used in generation facilities are inherently less robust than their counterparts in transmission and thus are more susceptible to EMP disruption. They are highly computer controlled which further exacerbates their risk to EMP. Yet at the

same time, they have trained personnel on site who with proper training, procedures, and spare parts, can greatly assist in restoration. System-level protection assurance is more complex due to the need for multiple systems to function in proper sequence. Lead times on generation components are even longer than for major transmission components. Existing coal plants make up nearly half the Nation's generation, but they generally have the most robust control systems with many remaining electro-mechanical controls still in operation. Natural gas-fired combustion turbines and associated steam secondary systems represent the newest significant contribution to the generation. These are mostly all modern electronic- and computer-based control and protective systems and are considered very vulnerable to EMP. Their fuel systems are not on site and will also be interrupted due to EMP. Nuclear plants have many redundant and fail-safe systems, but they too are very electronically controlled. The key difference with nuclear power plants is the extensive manual control capability and training, making them less vulnerable than the others. Hydroelectric is the next substantial generation element and is the most robust, although its older mechanical and electromechanical controls are being replaced at a rapid rate. Black start generation is normally quite secure but start and frequency controls will need to be protected from EMP. The highest priority generation assets are those needed for black start, but all are critical for restoration of any meaningful service.

- ◆ *Assure protection of high-value transmission assets*—Ability to withstand EMP must be assured at the system level. Priority for protection is on the highest voltage, and on the highest power units serving the longest lines; these require the most time to replace and are the most vulnerable in the absence of normal protections due to E1 and provide the major flow and delivery of power. Provisions must be made for the protection of large high-value assets such as transformers and breakers against the loss of protection and sequential subsequent impacts from E2 and E3 creating damage. E3 ground-induced current impacts are important from an industry standpoint since they can occur beyond E3 due to the risk of large, 100-year geomagnetic solar storms. For E3 this could include adding either permanent or switchable resistance to ground in the neutral of large transformers. This protection would then be available upon notice of the onset of a solar storm or sufficient threat of EMP attack. Thus it provides a simple expedient that does not compromise performance under normal operation. Due to the interconnected nature of the grid and to the need for that connectivity to enable recovery, the likelihood of a blackout lasting years over large portions of the affected region is substantial with damage to these high-value components. The islanding of the system through nonsynchronous connections may help reduce the E2 and E3 impacts by shortening the long line coupling in some instances.
- ◆ *Assure sufficient numbers of adequately trained recovery personnel*—Expand levels of manpower and training as they are otherwise limited to only that needed for efficient normal power operation that is highly and increasingly computer aided. Industry and government must work together to enhance recovery capability.
- ◆ *Simulate, train, exercise, and test the recovery plan*—Develop two or three centers for the purpose of simulating EMP and other major system threatening attacks. Develop procedures for addressing the impact of such attacks to identify weaknesses, provide training for personnel and develop EMP response training procedures and coordination of all activities and appropriate agencies and industry. While developing response plans, training and coordination are the primary purpose, identifying vulnerabilities through “red team” exercises is also important for identifying, prioritizing, and recti-

fying weaknesses. The centers would each focus on one of the three main integrated electrical networks — Eastern Grid, Western Grid, and Texas. These centers may be able to effectively utilize facilities such as the TVA bunker and the BPA control center in order to conserve resources and achieve rapid results. DOE facilities and other no longer utilized facilities should also be examined. Develop simulators to train and develop procedures similar to the airline industry. Exercising black start will require indemnification of power providers.

- ◆ *Develop and deploy system test standards and equipment*—Test and evaluate the multitude of system components to ensure that system vulnerability to EMP is identified and mitigation and protection efforts are effective. Device-level standards and test equipment exist for normal power line disturbances (EMC standards), but protection at the system level is the more important goal. System-level improvements such as isolators, line protection, and grounding improvements will be the most practical and least expensive in most cases rather than replacement of individual component devices.
- ◆ *Establish installation standards*—More robust installation standards must be identified and implemented as appropriate — such as short shielded cables, circumferential grounding, arrestors on leads, surge protectors, and similar activities. These should include more robust system standards — such as proximity to protected device, no commercial off-the-shelf (COTS) computers in mission critical roles and similar matters. In some instances, these will qualify as add-ons and replacements during the early period initiatives. The Government should complete the testing and evaluation work that the Commission initiated to set hardening standards for electric power protective systems. Government should provide fiscal assistance to industry in implementing the needed hardening solutions.

### **Cost and Funding of Selected Initiatives**

It must be noted that the very wide variety of components; installation techniques; local system designs; age of components, subsystems, and controls located within buildings or exposed; and so forth all drastically affect the type and expense for implementing the recommended initiatives. Internal DHS and other governmental costs are assumed to be absorbed. A significant portion of the labor to affect the modifications is already in place. Often the modification will be part of a program for repair, replacement and modernization that is continuing regardless of the EMP mitigation program. The addition of non-synchronous connection capability once defined is a contract function coupled with at-site staffing and control system interfaces. All of this effort factors into the cost estimates and results in fairly wide ranges in most instances. Only the costs for some of the larger or more system-specific initiatives are estimated here (in 2007 dollars).

- ◆ There are several thousand major transformers and other high-value components on the transmission grid. Protective relays and sensors for these components are more than that number but less than twice. A continual program of replacement and upgrade with EMP-hardened components will substantially reduce the cost attributable uniquely to EMP. Labor for installation is already a part of the industry work force. The estimated cost for add-on and EMP-hardened replacement units and EMP protection schemes is in the range of \$250 million to \$500 million.
- ◆ Approximately 5,000 generating plants of significance will need some form of added protection against EMP, particularly for their control systems. In some instances the

fix is quite inexpensive and in others it will require major replacements. The estimated cost is in the range of \$100 million to \$250 million.

- ◆ The addition of nonsynchronous interfaces to create subregion islands is not known with reasonable certainty, but it might be in the order of \$100 million to \$150 million per island. The pace of creating islands and their priority will be established by DHS in consultation with NERC and FERC. Moving to at least six or more fairly rapidly is a fair assumption. There will be annual operating costs of around \$5 million per island.
- ◆ The simulation and training centers are assumed at three — one for each interconnect — for a cost in the range of \$100 million to \$250 million plus annual operating costs of around \$25 million per year.
- ◆ Protection of controls for emergency power supplies should not be too expensive since hard-wired manual start and run capability should be in place for many, which is adequate. Furthermore, the test, adjust, and verification will be carried out by the entity that owns the emergency power supply as part of normal operating procedures. Retrofit of protective devices such as filters might be accomplished at a cost of less than \$30,000 per generator for newer generators with vulnerable electronic controls. Hardening the connection to the rest of the facility power system requires a protected internal distribution system from the backup generator.
- ◆ Switchable ground resistors for high-value transformers are estimated to cost in the range of \$75 million to \$150 million.
- ◆ The addition of new black start generation with system integration and protected controls is estimated to cost around \$12 million per installation. Probably no more than 150 such installations will need to be added throughout the United States and Canadian provinces. Adding dual fuel capability to natural gas-fired generation is done for the economic purpose of the owner, yet it has the same value as the addition of black start generation. The addition of fuel storage for the existing black start units is relatively small, about \$1 million each.
- ◆ The addition of emergency generation at the multitude of sites including fuel and transportation sites is probably around \$2 million to \$5 million each.
- ◆ The cost for monitoring, on a continuous basis, the state of the electric infrastructure, its topology, and key elements plus for assessing the actual EMP vulnerability, validation of mitigation and protection, maintenance, and surveillance data for the system at large cannot be estimated since it falls under many existing government-funded activities, but in any event, it is not considered significant.
- ◆ Research and development activities are a level-of-effort funding that needs to be decided by DHS. Redirection of existing funding is also likely to occur.
- ◆ Funding for the initiatives above is to be divided between industry and government. Government is responsible for those activities that relate directly and uniquely to the purpose of assuring continuation of the necessary functioning of U.S. society in the face of an EMP attack or other broadly targeted physical or information systems attack. Industry is responsible for all other activities including reliability, efficiency and commercial interests. Industry is also the best source for advice on cost effective implementation of the initiatives.





## Chapter 3. Telecommunications

### Introduction

Telecommunications provides the connectivity that links the elements of our society together. It is a vital capability that plays an integral role in the normal day-to-day routine of the civilian, business, and government sectors of society. It is a critical enabler for the functioning of our national financial infrastructure, as transactions representing trillions of dollars flow daily via telecommunications. It enables agencies of local, state, and federal government to discharge their duties. People can communicate on the go, almost anytime and virtually anywhere because of telecommunications, as exemplified by more than 100 million cellular subscribers in the United States (U.S.). Telecommunications provides a vital pathway between emergency response personnel in crisis situations. It has transformed, via the Internet and advances in technology, the way business and society in general operate. Downloading music and video content using the Internet instead of in-store purchases, using cell phones to interactively gather travel directions instead of using paper maps, and using remote sensors and video streams to send security information over a communications network to a central site for appropriate dispatch instead of using on-site security guards are examples of these changes.

Telecommunications can be thought of as:

- ◆ The mix of equipment used to initiate and receive voice, data, and video messages (e.g., cell phones and personal computers).
- ◆ The associated media (e.g., fiber optics and copper) and equipment (e.g., multiplexers) that transport those messages.
- ◆ The equipment that routes the messages between destinations (e.g., Internet Protocol [IP]-based routers).
- ◆ The basic and enhanced services offered by communications carriers such as AT&T, Verizon Wireless, and Comcast.
- ◆ The supporting monitoring and management systems that identify, mitigate, and repair problems that can impact performance of services.
- ◆ The supporting administrative systems for functions such as billing.

This chapter discusses civilian telecommunications. Among the main trends to consider in evaluating the impact of EMP on these telecommunications networks in the next 15 years are:

- ◆ The dramatic growth in the number of wireless networks and in the use of wireless services.
- ◆ Improvements in the technology and reliability associated with optical networks leveraging heavy fiber deployment (fiber is generally viewed positively in terms of EMP survivability).
- ◆ Shrinking work forces used in managing networks and an associated increase in dependence on automation and software “diagnostic smarts” to support maintenance, problem isolation and recovery, and other performance impacting functions.
- ◆ An architectural evolution toward a converged network in which voice, data, and video traffic are carried over the same network.

When fully implemented, this evolution to a converged network will represent a major change-out of the equipment that existed in the 1990s, and that still exists, in the U.S.

telecommunications network. Thus, it represents an opportunity for EMP hardening considerations to be included as the transition occurs.

Telecommunications service providers have proclaimed that carrying voice, data, and video together over converged networks is an underpinning of their strategic directions. Service providers point to the fact that traffic residing on embedded, older technology will be transitioned to this new converged network within financial and regulatory constraints.<sup>1</sup> While this converged network evolution has begun, it is expected to continue for an additional decade or more.

The reason for a lengthy transition can be better understood by reviewing some historical factors related to the U.S. telecommunications network. Several factors led to traffic being carried by separate networks, including differences in the characteristics of voice, data, and video traffic; the relative dominance in the amount of voice traffic over data and video; and the technological state of the carrier network equipment.

With respect to traffic characteristics:

- ◆ Voice communications generally are characterized by real-time interactions with typical durations of a few minutes.
- ◆ Data communications tend to occur in bursts and may consume large amounts of bandwidth during these bursts. Data communications users often access networks for long holding times that may range into hours.
- ◆ Video traffic typically is characterized by high-bandwidth, long-duration, one-way transmission such as distributing cable TV content to viewers with lower-bandwidth traffic sent from the subscriber to the service provider, for example, to signal the selection of a specific on-demand program.

With respect to traffic mixes:

- ◆ As the 1990s progressed, the growth of data traffic exploded, fueled in large part by Internet usage. Data communications growth is continuing at a rapid pace, while growth in voice has remained relatively flat. Some estimates have data traffic already exceeding voice traffic beginning around the year 2000.
- ◆ The growth in data communications traffic has made it more fiscally attractive to find technological solutions that avoid the expense of maintaining separate voice and data networks.

With respect to technology evolution:

- ◆ Voice communications over the past decade have been handled primarily by carrier equipment called digital circuit switches. The switches are engineered based on statistical usage of the network that assumes not all of the individual users, traditionally in the thousands, served by those individual switches will try to gain access simultaneously. These switches, of which several thousand are deployed, were not designed to effectively handle the characteristics of data and video traffic.
- ◆ Router technology has evolved rapidly. Advances in protocols that support assigning quality of service (QoS) requirements for different traffic mixes and greater processing speed and capacity have provided solutions for handling voice, data, and video using a common set of equipment.

---

<sup>1</sup> Wegleitner, Mark, Verizon, Senior Vice President, Broadband Packet Evolution, Technology, 2005.

- ◆ Service providers implement new technologies slowly. This is prudent given the complexity of the networks in question and a desire to prove-in technologies and fine-tune network management procedures prior to wide-scale deployment.

### Telecommunications Support During Emergencies

There is a recognition at the highest levels of government and industry that telecommunications plays a critical role, not only in the normal day-to-day operations of society, but also in reconstituting societal functions and mitigating human, financial, and physical infrastructure losses during man-made and natural disasters. This has led to government and industry partnering to codify processes, organizational structures, and services to address these disasters. Among these codifications are the National Communications System (NCS) and a set of services known as National Security and Emergency Preparedness (NS/EP) services.

The NCS was established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*.<sup>2</sup> These functions include administering the National Coordinating Center for Telecommunications (NCC) to facilitate the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities under all crises and emergencies; developing and ensuring the implementation of plans and programs that support the viability of telecommunications infrastructure hardness, redundancy, mobility, connectivity, and security; and serving as the focal point for joint industry-government and interagency NS/EP telecommunications planning and partnerships.

With respect to the NS/EP telecommunications services, a set of evolving capabilities exist for:

- ◆ Prioritizing telephone calls through the wireline and wireless networks during time intervals when call volumes are excessive and facilities may be degraded.
- ◆ Giving priority to restoring emergency and essential services that may be damaged or degraded.
- ◆ Rapidly getting new telecommunications connections into operation.
- ◆ Keeping carriers communicating with government and one another on an on-going basis during crises events.

NS/EP-related definitions are noted below.

NS/EP Definitions
<i>NS/EP Telecommunications Services</i> —Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States. ( <i>Telecommunications Service Priority [TSP] System for National Security Emergency Preparedness: Service User Manual, NCS Manual 3-1-1, Appendix A, July 9, 1990</i> )
<i>NS/EP Requirements</i> —Features that maintain a state of readiness or respond to and manage an event or crisis (local, national, or international), which causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the NS/EP posture of the United States. (Federal Standard 1037C)
<i>Emergency NS/EP and Essential NS/EP</i> —Emergency NS/EP telecommunication services are those new services that are “so critical as to be required to be provisioned at the earliest possible time without regard to the costs of obtaining them.” An example of Emergency NS/EP service is federal government activity in response to a Presidential declared disaster or emergency. Telecommunications services are designated as essential where a disruption of “a few minutes to one day” could seriously affect the continued operations that support the NS/EP function. (Federal Register/Vol. 67, No. 236, December 9, 2002/Notices)

<sup>2</sup> Executive Order 12472, April 3, 1984.

These NCS and NS/EP services are capabilities that would be drawn upon in an EMP event, and they will evolve as the U.S. telecommunications network evolves. This commitment to evolution has been reinforced, for example, by testimony from Frank Libutti (Undersecretary, Information Analysis and Infrastructure Protection, Department of Homeland Security) before the United States Senate Committee on Appropriations in 2004:

The NCS is continuing a diverse set of mature and evolving programs designed to ensure priority use of telecommunications services by NS/EP users during times of national crisis. The more mature services—including the Government Emergency Telecommunications Service (GETS) and the Telecommunications Service Priority (TSP)—were instrumental in the response to the September 11 attacks. FY 2005 funding enhances these programs and supports added development of the Wireless Priority Service (WPS) program and upgrades to the Special Routing Arrangement Service (SRAS). Specifically, priority service programs include: (1) GETS, which offers nationwide priority voice and low-speed data service during an emergency or crisis situation; (2) WPS, which provides a nationwide priority cellular service to key NS/EP users, including individuals from Federal, state and local governments and the private sector; (3) TSP, which provides the administrative and operational framework for priority provisioning and restoration of critical NS/EP telecommunications services. In place since the mid-1980s, more than 50,000 circuits are protected today under TSP, including circuits associated with critical infrastructures such as electric power, telecommunications, and financial services.; (4) SRAS, which is a variant of GETS to support the Continuity of Government (COG) program including the reengineering of SRAS in the AT&T network and development of SRAS capabilities in the MCI and Sprint networks, and; (5) the Alerting and Coordination Network (ACN) which is an NCS program that provides dedicated communications between selected critical government and telecommunications industry operations centers.<sup>3</sup>

### EMP Impact on Telecommunications

To aid in understanding the impact of EMP on telecommunications, **figure 3-1** provides a simplified diagram of a telecommunications network.

Service subscribers communicate through a local node. For example, a cellular subscriber communicates through a cell tower controlled by a cellular base station. If communication is with a party located on another local node, the communications traffic may be routed through the backbone to the distant local node for delivery to the other party. The backbone connects to thousands of local nodes and in doing so serves a transport and routing function to move voice, data, or video traffic between or among the communicators. It consists of a mix of equipment that provides high-speed connectivity between the local nodes. In an actual network if there is sufficient traffic between two local nodes, they may be directly connected by transmission media such as fiber links. **Figure 3-1** shows some network equipment, such as a digital switch and a network router. The control network collects information statistics from the equipment in the local nodes and

<sup>3</sup> [http://www.globalsecurity.org/security/library/congress/2004\\_h/040302-libutti.htm](http://www.globalsecurity.org/security/library/congress/2004_h/040302-libutti.htm).

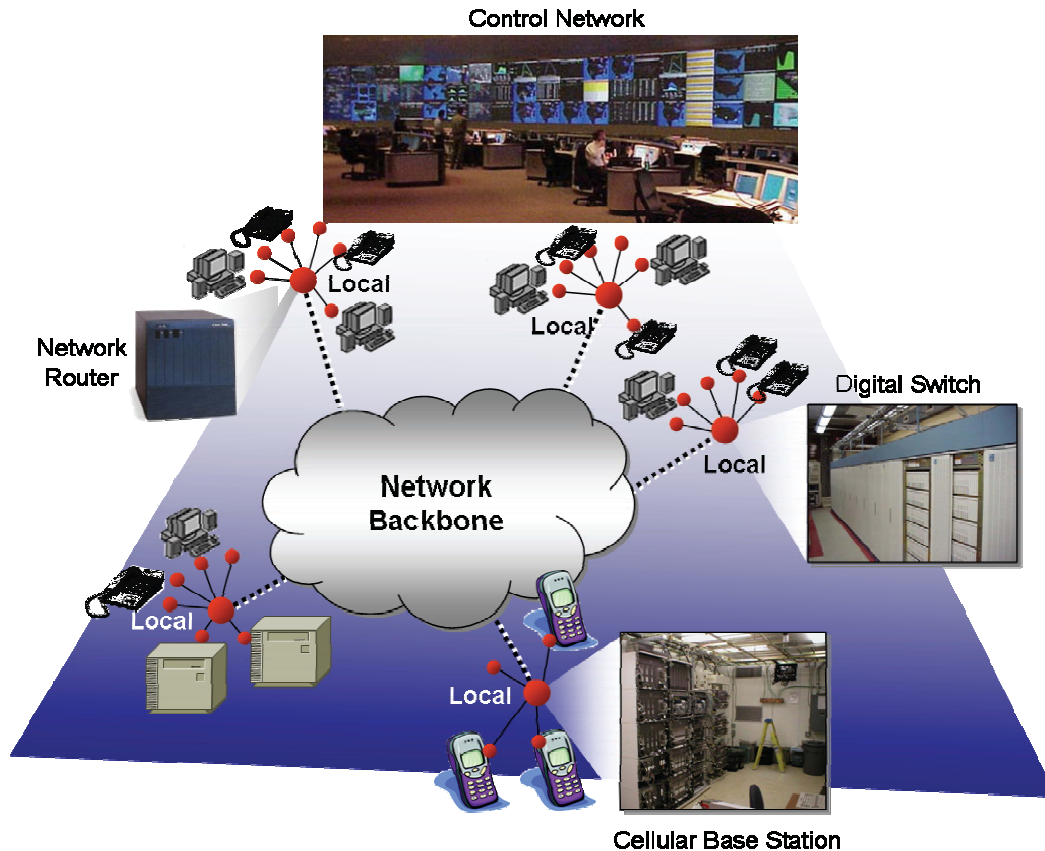


Figure 3-1. Generic Telecommunications Network Architecture

backbone that help manage the network's performance. The backbone has been the main focus of industry in deploying components of the converged network to date, and it is the furthest along with respect to the converged network vision.

A set of first-order assumptions drove the analytical assessment of EMP impacts on telecommunications:

- ◆ In a crisis, voice services will be viewed as critical, with the percent of call attempts completed as a key metric.
- ◆ The backbone, as depicted in **figure 3-1**, is where the greatest influx of new equipment has been deployed. This is newer-vintage, expensive, high-end routing and transport equipment connected by fiber optics. An assumption is that the equipment will be highly survivable up to high E1 EMP levels and perhaps will experience only transient effects at those levels, but this needs to be verified with further testing.
- ◆ The local nodes will be replaced with equipment supporting the converged network vision, but this change-out will continue beyond the time frame examined in this Commission study. Commission-sponsored testing provided insights into the performance of the new equipment that is being incorporated into the converged network. Among the current local node equipment are digital circuit switches and other equipment that have been tested and analyzed as part of a prior assessment of E1 EMP on telecommunications conducted in the early 1990s.<sup>4</sup> In this study, circuit switch

<sup>4</sup> For example, Network Level EMP Effects Evaluation of the Primary PSN Toll-Level Networks, Office of the Manager: NCS, January 1994.



manufacturers noted they would be incorporating equipment changes to address a majority of the items shown to be susceptible to E1 EMP in the products tested, and the Commission assessments assume this to be the case.

Keeping these factors in mind, the Commission focused its analytical efforts on customer premises equipment (CPE), the subsequent impact on demand levels at the local nodes and local node equipment, and the subsequent ability to complete calls assuming a robust backbone.

On the demand side, call origination electronic assets have the potential for EMP disruption or damage. A key issue is whether EMP will impact the operation of telephones, cell phones, and computer systems (like those shown in **figure 3-1**) and, as such, reduce the demand placed on assets in the local and backbone elements that move information between information senders and receivers.

The major elements of the civilian telecommunication network are electronic systems with circuit boards, integrated circuit chips, and cable connections such as routers that switch and transport information between users of the network (e.g., transport phone calls). Like the equipment that generates demand on the network, these electronics have an inherent vulnerability to EMP threats. The majority of these critical switching and transport assets that are part of the local and backbone nodes in **figure 3-1** are housed in Central Offices (COs). Typically COs are windowless concrete buildings. Sometimes equipment used to provide service to end users is housed in Controlled Environmental Vaults (CEV). These are smaller structures that provide environmental control similar to that of a CO. Wireless base stations supporting cellular communications are housed in structures similar to CEVs. Finally, some equipment such as that used to provide high-speed Internet service may be installed in small cabinets and enclosures without environmental controls.

Regardless of the installation location, telecommunications equipment and the facilities that contain them follow strict rules and requirements to protect against natural or unintentional electromagnetic disturbances, such as lightning, electromagnetic interference, electrostatic discharge, and power influences on telecom cables. Typical protection techniques include grounding, bonding, shielding, and the use of surge protective devices. However, an EMP attack exhibits unique characteristics, such as rapid rise-time transients, and the existing protection measures were not specifically intended for or tested against EMP.

Given these network characteristics, some factors that contribute to mitigating EMP effects on telecommunications are:

- ◆ Industrywide groups that systematically share best practices and lessons learned to improve network reliability, such as the Network Reliability and Interoperability Council (NRIC).
- ◆ Availability of NS/EP telecommunications capabilities.
- ◆ Volume, geographic diversity, and redundant deployment of telecommunications equipment assets, coupled with wireline, wireless, satellite, and radio as alternative means for communications.
- ◆ Deployment of fiber-optic technology within telecommunications carrier networks.
- ◆ Use of standard bonding and grounding practices for telecommunications equipment deployed in carrier networks.

- ◆ Historical performance of terrestrial carrier networks in electromagnetic events such as lightning and geomagnetic storms.

The Commission sponsored testing and analytical efforts that led to the conclusion that an EMP attack would disrupt or damage a functionally significant fraction of the electronic circuits in the Nation's civilian telecommunications systems in the geographic region exposed to EMP. Cellular networks are seen as being less robust to EMP than landline networks due to a combination of the higher susceptibility of cellular network equipment to damage and more limited backup power capacity at cell sites than at counterpart landline network equipment sites.

The analysis suggested that damage to telephones, cell phones, and other communications devices would not be sufficient to curtail higher than normal call volumes on the civilian telecommunications network after exposure to either low or high E1 EMP levels. As such, the remaining operational network would be subjected to high levels of call attempts for some period of time after the attack, leading to degraded telecommunications services. Key government and nongovernment personnel will need priority access to use public network resources to coordinate and support local, regional, and national recovery efforts. This will be especially problematic during the interval of severe network congestion. Services such as GETS will be crucially important during these periods of high call demand.

The Commission's expectation is that the impact of a low E1 EMP level exposure would be dominated by the inability to handle the spike in call traffic on landline networks, because the direct impacts on equipment are expected to be largely transient and short term in nature (minutes to hours) with minimal manual restoration. For cellular networks, the impact will be greater (minutes to days) due to the expected levels of manual recovery, more limited backup power at cell sites, and the large number of cellular base stations that serve as key controllers of communications between cell towers and cell phones. The results of limited testing on cellular base stations indicate EMP vulnerabilities that require further examination.

As noted in the electric power section of the Commission report, the loss of portions of the power grid is likely, even for a relatively low-level EMP attack. The longer-term performance of the public telecommunications network and associated NS/EP services will depend, therefore, on the use of backup power capabilities and the rapidity with which primary power can be restored. To offset a loss of electric power, telecommunication sites now use a mix of batteries, mobile generators, and fixed-location generators. Typically, these have 4 to 72 hours of backup power available on-site and thus will depend on either the resumption of electrical utility power or fuel deliveries to function for longer periods of time. A short-term electric power grid outage (less than a few days) would not cause a significant loss of telecom services due to the existence of power backup systems and best practices supporting these critical systems.

In the case of high amplitude E1 EMP level exposures, spikes in call traffic, coupled with a mix of transient impacts and damage requiring manual network equipment restoration, will result in degraded landline and cellular communications on the order of days to weeks. As in the case of low E1 levels, longer-term impacts from power outages could extend the period and severity of the degradation.

General results from the Commission's EMP analysis received concurrence from the NCS as noted below.

**Senate Testimony (March 2005)**

In March 2005 testimony before a U.S. Senate subcommittee (Terrorism and the EMP Threat to Homeland Security, Subcommittee on Terrorism, Technology, and Homeland Security, March 8, 2005), the Acting Director of the NCS noted that “Just last year, the NCS also actively participated in the congressionally-chartered *Commission to Assess the Threat from High Altitude Electromagnetic Pulse* (the 2004 EMP Commission) that examined and evaluated the state of the EMP threat at present and looking 15 years into the foreseeable future. The Commission’s Report, delivered last July, concludes that EMP presents a less significant direct threat to telecommunications than it does to the National Power grid but would nevertheless disrupt or damage a functionally significant fraction of the electronic circuits in the Nation’s telecommunications systems in the region exposed to EMP (which could include most of the United States). The NCS concurs with this assessment.”

**Analysis Approach**

To estimate the impact of an EMP attack on the civilian telecommunications network, the following major tasks were performed:

- ◆ Reviewed lessons learned with respect to telecommunications critical dependencies and susceptibilities from past studies of events, such as major disasters and Year 2000 (Y2K).
- ◆ Visited telecommunications facilities to get “ground truth” insights into possible areas of EMP susceptibility and for data such as equipment layouts to support illustrative testing of telecommunications equipment.
- ◆ Reviewed past test data and performed illustrative testing of wireline and cellular communications devices such as cell phones and network equipment such as network routers to determine EMP susceptibilities.
- ◆ Developed models of telephone network restoration processes and network call processing associated with alternative EMP scenarios using subject matter expert judgment, illustrative test data, and augmentation of existing models to estimate degradation levels for networks. Network statistics such as call completion levels used to estimate degradation were generated for users, assuming they were not using NS/EP services such as GETS.

**Analysis Approach—Lessons Learned**

From interviews and reviews of lessons learned from past outage events, the following issues were identified that helped shape Commission recommendations and provided input for the testing and modeling activities:

- ◆ Y2K contingency planning and past outage events, such as the Hurricane Katrina blackout, point to the need for a functioning voice communications network in an emergency situation to support restoration efforts for multiple critical infrastructures. For example, with respect to managing the power grid, reference material associated with Y2K preparations noted, “The principal strategy is to operate using a manual transfer of a minimum set of critical information ... electric systems must provide sufficient redundancy to assure voice communications over a geographic area that addresses its critical facilities and interfaces to neighboring systems and regional centers.”<sup>5</sup>
- ◆ Conditions that would lead to multi-day unavailability of power remain a principal concern of telecommunications providers. Extended power outages will exacerbate attempts to repair damage and lead to fuel shortages that end up taking network capacity off-line. This concern was reinforced by Hurricane Katrina and by the August

<sup>5</sup> <http://www.y2k.gov/docs/infrastructure.htm>.

2003 Northeast Power Outage. The latter was a key topic of the August 27, 2003, NRIC meeting.

- ◆ A high level of call attempts on both wireline and wireless networks will follow an EMP attack, thereby reducing the effectiveness of voice communications for some time period. At least four times the normal call traffic will likely be experienced by these networks. In previous disasters, these high levels generally lasted for 4 to 8 hours and remained slightly elevated for the first 12 to 24 hours after the event. The spike in call volumes results in callers experiencing problems in successful call completion. Additionally, callers may experience conditions such as delayed dial tones or “all circuits busy” announcements. As an example, the high blocking levels experienced by callers on cellular networks on September 11, 2001, in Washington, D.C., and New York City are shown in **figure 3-2** as call attempts rose to levels as high as 12 times normal.<sup>6</sup>

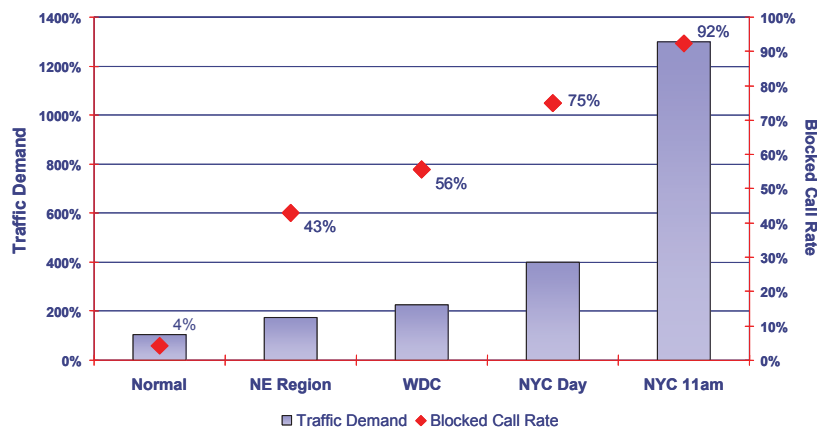


Figure 3-2. September 11, 2001, Blocked Call Rate—Cellular Networks

- ◆ As previously noted, concerns over the ability of key personnel to get calls through the public telecommunications network in a disaster was one of the catalysts for services development that occurred under the leadership of the NCS. GETS and WPS are services intended for use in emergency conditions to improve the probability of key personnel completing calls even when wireline and wireless network are under extremely heavy call loads. These services will be leveraged during an EMP event, but their benefits for subscribers are mitigated when local equipment requires manual recovery to be functional. Based on test results, this manual recovery requirement for cellular base stations is of particular concern.
- ◆ Maintenance and control functions will be critical to restoration and recovery efforts, as they are used by telecommunications carriers to alleviate the overload conditions and identify areas of damage within the network to hasten recovery efforts. For the general populace without access to NS/EP services, if massive call attempts tie up network resources there would be minimal circuits available to dial out and potentially reduced capability to reach 9-1-1 services. To help alleviate this, personnel in a Network Management Center (see **figure 3-3**) could issue a command to the carrier network for “call gapping” through a few quick keystrokes on a personal computer. Through this command, some percentage of calls would be stopped at the originating

<sup>6</sup> Aduskevicz, P., J. Condello, Capt. K. Burton, Review of Power Blackout on Telecom, NRIC, August 27, 2003, quarterly meeting.

switch and thus free up resources that would be needed for dialing out. Testing conducted as part of the previously referenced NCS-sponsored assessment indicated that some physical damage to circuit switch components linking to these network management facilities would occur, even at very low transient levels. This damage would reduce the ability of recovery efforts to bring systems up to full capacity and affect the ability to remotely implement procedures to address EMP-induced network problems.

#### *Analysis Approach—Collecting Ground Truth*

Prior to conducting testing on equipment, visits were made to carrier facilities to verify some of the assumptions regarding equipment layouts that were used in the test configurations. Sites containing wireline network switching and transport equipment, cellular network switching and transport equipment, and Network Management Center equipment were visited. Features such as cable lengths and bonding and grounding practices and issues such as policies for stockpiling spares were explored during these visits. In addition, discussions were held with personnel involved in telecommunications equipment installation activities, technical requirements development for electromagnetic effects protection, and network monitoring and control activities to vet assumptions made in the equipment testing and modeling activities. **Figure 3-4** shows cellular network base station equipment photographed during one of the visits.

**Figure 3-5** is a photo of router equipment used to collect performance information from carrier equipment and transmit it to a Network Management Center, such as the one in **figure 3-3**.

Based on the collected data, a process for network restoration was developed considering the wide mix of assets that could be affected in an EMP event. The restoration process was reviewed with experts who had been involved in large restoration efforts, including personnel charged with developing software systems to expedite network recovery. These reviews helped augment the restoration process model. This process was used in developing recovery timelines generated in the modeling and simulation activity.

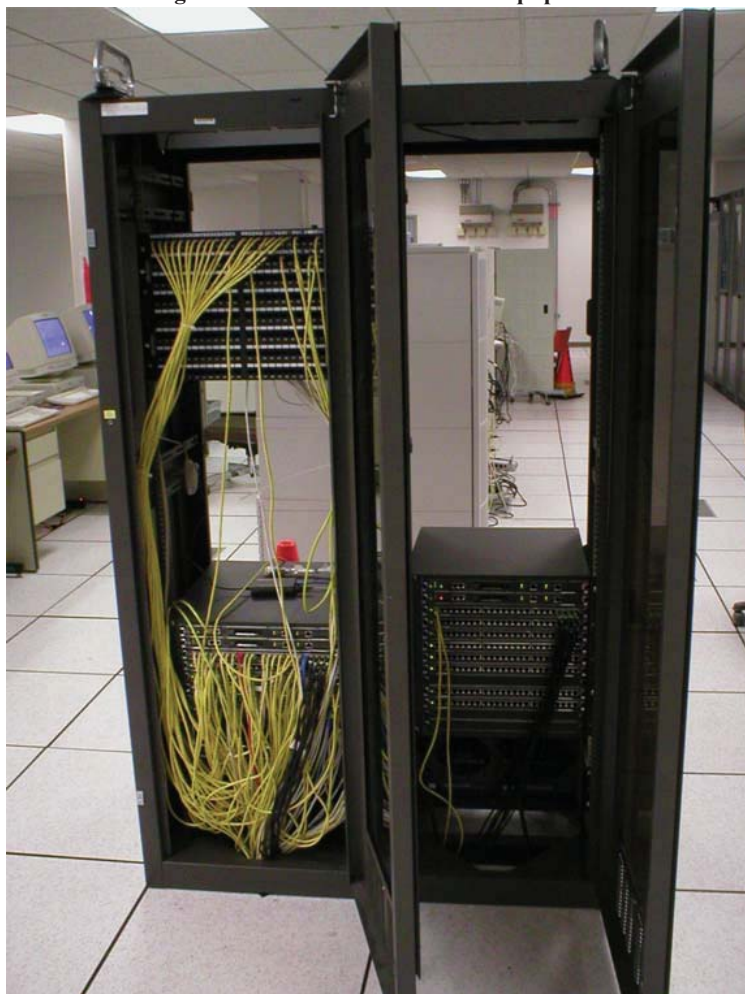


**Figure 3-3. Example Network Management Facility**





**Figure 3-4. Cellular Base Station Equipment**



**Figure 3-5. Routers Collecting Network Management Data**

### *Analysis Approach—Testing for EMP Effects on Telecommunications Networks*

Using the lessons learned and ground truth data described previously, a test plan was developed that focused most heavily on the effects of EMP on voice communications and the associated maintenance and control networks that would support recovery and restoration efforts. Consistent with this, testing activities focused on communications devices and switching and routing equipment expected to play a critical role in supporting future voice communications and on computing equipment supporting the collection of data used for network traffic management. E1 was considered as the primary source of EMP effects on carrier equipment under the assumption that long transport lines within carrier telecommunications networks have moved to fiber instead of copper. We also recognized the growing use of fiber within close proximity to home and business establishments. In accordance with these assumptions, the communications carrier network equipment testing focused on assets that would be considered part of the local nodes in **figure 3-1**.

Prior test data on digital switches, routers, computers, and related equipment were reviewed. For example, during the 1980s and early 1990s, the NCS sponsored testing on major telecommunications switches and transport equipment. The test effort conducted on behalf of the EMP Commission was designed to complement the data available in previously discussed NCS technical reports and other data sources. The test data provided information on the behavior of particular pieces of equipment and was subsequently used to model the impact of an EMP attack on the telecommunications network infrastructure and the recovery process. In addition to network equipment, CPE such as basic telephones and cell phones were tested, as the level of traffic on the public telecommunications networks would be affected by the CPE's EMP survivability. **Table 3-1** lists the telecommunications assets tested at multiple government and commercial facilities, including a rationale for why they were selected. A mixture of continuous wave immersion (CWI), pulse current injection (PCI), and free field illumination tests was used. **Figure 3-6** depicts testing that was conducted at a cellular base station at Idaho National Laboratory (INL). Free-field illumination testing was conducted on equipment covering each of the areas in **table 3-1** (except for cellular network carrier switching equipment [see **figure 3-6**]). The equipment tested included a softswitch, cordless phones, cellular phones, computing servers, Ethernet switches, and routers.

During the testing, in cases where impacts were observed, some were transient in nature, for example, auto-rebooting of softswitch equipment, while some testing resulted in permanent equipment damage and required manual recovery via replacement of components (for example Ethernet card replacement) to address performance degradation.

**Table 3-1. Telecommunications Equipment Tested**

Items	Importance
Corded Phones, Cordless Phones, Cell Phones	Key devices used for voice communications. The level of demand placed on the public telecommunications network will be impacted by the equipments' operational state.
Computing Servers, Secure Access Devices	These computers house software supporting key management and control functions (Network Fault and Traffic Management) critical to network recovery efforts. Since these systems may have to be accessed remotely in an emergency, secure access devices that generate passwords are used to gain access to them.
Routers, Ethernet Switches	Critical equipment supporting the routing of network control and status information between network elements and the facilities and computer systems responsible for their management.

**Table 3-1. Telecommunications Equipment Tested (continued)**

Items	Importance
Softswitches, Gateways	Key equipment being integrated into public networks to support the transmission of voice, data, and video over IP-based technology. This equipment is replacing the digital circuit switches that are part of the local nodes shown in <b>figure 3-1</b> .
Mobile Switching Centers, Base Stations, Base Station Controllers	Major operational components of cellular networks that are used to transmit cellular calls.
Cable Modem Termination System (CMTS), Cable Modems	Cable companies are moving aggressively into telecom, and cable modems are heavily used by customers to access the cable network for communications. The CMTS converts the data signals from cable modems to an Internet Protocol. Trends point to the increased use of routers, Ethernet switches, softswitches, and gateways to route communications traffic.

**Figure 3-6. Cellular Network Testing at INL****Figure 3-7. Testing at NOTES Facility**

**Figure 3-8** shows examples of some of the smaller items tested at the NOTES facility.





Figure 3-8. Secure Access Card and Cell Phones

#### *Analysis Approach—Modeling and Simulation of EMP Effects*

To develop a view of the system effects that would be caused by an EMP attack, a systematic approach was used in the modeling and simulation effort. The analysis leveraged the Commission-sponsored testing just described, as well as prior equipment testing results. Initially, a telecommunications network performance modeling approach for generating call completion levels given degradation assumptions in wireline and wireless networks was developed for the continental United States. The major assumption in this modeling was that the key area of degradation would be local nodes in the carrier networks (for both wireline and cellular networks). As shown in **figure 3-1**, local nodes are equipment such as the digital circuit switches and cellular base station equipment that provide callers with entry into these wireline and cellular telecommunications networks. Impacts on local nodes could inhibit local calls, as well as prohibit connections to the backbone network that provides for more geographically dispersed communications. Positive trends in the direction of EMP survivability for backbone communications are due to increased routing diversity coupled with heavy fiber deployment, suggesting that a local focus is reasonable in terms of first-order effects.

Following this logic, the modeling steps included:

1. Generate a case study using weapons detonation scenarios that produce electromagnetic field levels modeled over selected geographic regions of the United States and model the impact on network performance (e.g., call completion levels) given the degree of network upset expected to be caused initially by the EMP event. We included transient or self-correcting effects and effects that require human action to correct. The model incorporated past test results from NCS studies and new testing of the equipment listed in **table 3-1**, using assumptions about the types and configurations of equipment that would be deployed in affected areas. The starting point for equipment types was industry databases identifying equipment deployed in telecommunications networks. This was augmented with subject matter expert discussions.
2. Apply generic methods and procedures incorporated in the network restoration process noted earlier to generate recovery times for network equipment. Inputs include engineering assumptions on equipment damage levels, availability of repair personnel, availability of network management and control functions, availability of electric power, and other factors.

3. Use the recovery times to model placing equipment back in service and iteratively estimate network performance levels over time using the network performance model.

The following are illustrative results generated from among scenarios of interest identified by the Commission. **Figures 3-9 through 3-11** show originating call completion levels in the eastern United States for the average combined wireline and wireless calls after an EMP event. Time period categories in these figures include immediately following, 4 hours after, and 48 hours after the EMP event. The results displayed incorporate longer restoration times for cellular equipment, driven in part by levels of manual recovery. **Figure 3-12** shows the recovery curve during the 10-day period following the attack. This is the estimated time period to regain pre-event performance, absent other infrastructure interdependency impacts such as long-term power outages. The shaded circles indicate EMP field-level isocontours generated by the weapon. For example, in **figure 3-9**, the geographic area most negatively impacted has estimated call completion levels of roughly only 4 percent, while the area outside the range of the direct effects has a 73 percent call completion level estimate.

The reason for the 73 percent level is that callers outside the directly affected areas are unable to make calls into the affected areas due to equipment disruptions in those areas, coupled with network congestion and high call-retry levels.

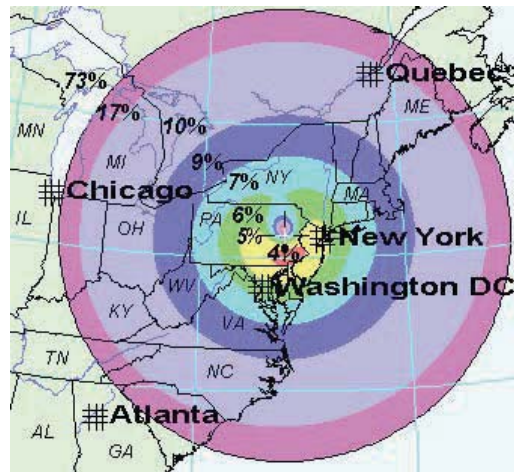


Figure 3-9. Percentage of Calls Completed Immediately After EMP Event

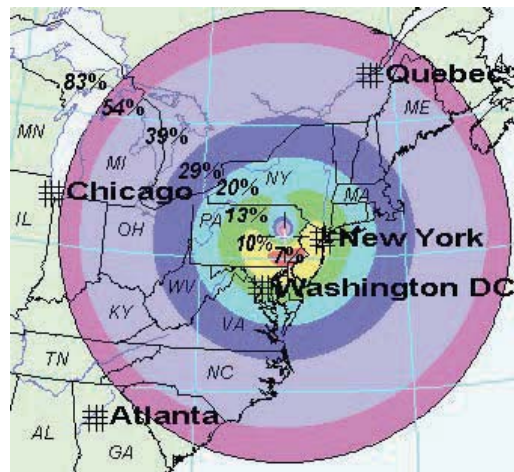


Figure 3-10. Percentage of Calls Completed 4 Hours After EMP Event



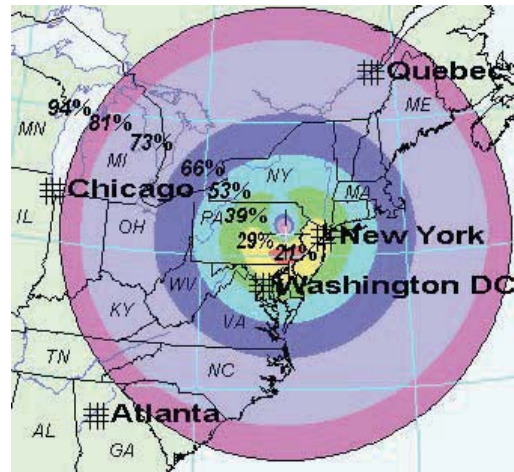


Figure 3-11. Percentage of Calls Completed 2 Days After EMP Event

The illustrative results in **figure 3-12** highlight the value of operational GETS and WPS capabilities given that the call completion levels noted in **figure 3-12** would be unacceptable for NS/EP functions during the critical early stages of an emergency. The analysis performed as part of this EMP Commission effort did not explicitly examine the performance of these NS/EP services in an EMP attack. The call completion levels in **figure 3-12** would be seen as likely lower bounds for these services for the scenarios of interest examined.

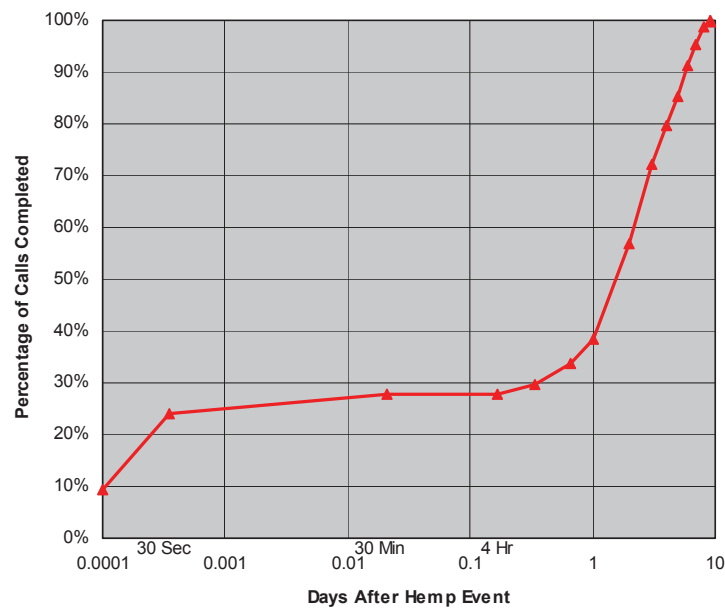


Figure 3-12. Percentage of Calls Completed at Time T  
(Logarithmic Time Scale)  
(Within EMP Contours)

The scenarios examined indicated that even in the case of minimal equipment damage, the functioning of NS/EP telecommunications services are critical to handling the spike in caller traffic expected to follow an EMP attack. This traffic tends to overwhelm the available telecom network capacity and results in degraded network performance. While operational experience exists with the current technologies that support NS/EP services, there is the need to make sure that NS/EP services operate effectively as new technolo-

gies, such as softswitches, are being introduced into the network. It is important to verify that this equipment will operate through an EMP attack under the stressful operating conditions that are anticipated in an emergency situation. The use of IP-related technology such as softswitches to support GETS and WPS services is at the initial point of deployment in local offices. Rigorous analysis is warranted prior to their major deployment to examine EMP survivability issues.

During sensitivity analysis, in the process of examining alternative cellular base station damage levels, an area of concern was identified within the cellular network system. Specifically, the area of concern was degradation of network performance due to EMP effects on critical databases, including the Home Location Registers (HLRs). HLRs contain key user information associated with cellular subscribers, such as account status and location. Within the wireless industry, the deployment approach to achieve HLR diversity (physical and geographic) is mixed. HLRs were not tested for susceptibility levels as part of the EMP Commission study, but using proxy numbers based on testing for circuit switching equipment, sensitivity studies show that it is possible to lose major calling areas in an EMP attack due to HLR degradation. In addition to EMP susceptibility testing, engineering polices and selective EMP hardening of these elements are options that should be examined in the future.

As noted in the Electric Power chapter, loss of portions of the power grid is likely, even for a relatively low-level EMP attack. Our analysis indicates that, in a relatively low-level EMP attack, the direct impact on public telecommunications networks is likely to be dominated by the inability to handle ensuing spikes in call traffic. In such cases, the direct effects on equipment are expected to be largely transient and short term in nature (minutes to hours) with minimal manual restoration needed. However, should widespread loss of primary power occur, the survivability of the telecommunications network and associated NS/EP and other services will depend on the use of backup power capabilities and the rapidity with which primary power can be restored. Most public telecommunications equipment has a mix of battery, mobile generator, and fixed generator support if primary electric power is lost. A short-term loss of the electric power supporting most telecommunications networks today would not cause a major loss of telecom services. This is due to the existence of power backup systems and best practices supporting these critical systems that could sustain telecom services during short-term power outages.

The situation becomes more serious if the power outages are long term and widespread. In such cases, the likely loss of major telecommunications facilities would significantly reduce NS/EP services. A majority of residential telephones today depend on power from local central offices, which would be lost once the backup power at those offices is depleted. Other residential telephones also require commercial power to function. Thus, citizen ability to access 9-1-1 call centers would be a major concern in an extended power outage situation.

Hurricane Katrina in August 2005 damaged cell phone towers and radio antennas. The prolonged blackout resulting from Katrina exhausted the fuel supplies of backup generators servicing emergency communications. Consequently, emergency communications for police, emergency services, and rescue efforts failed. Significantly, these same nodes so critical to emergency communications—cell phone towers and radio antennas—are vulnerable to EMP attack. A protracted blackout resulting from an EMP attack would also exhaust fuel supplies for emergency generators, just as occurred during Hurricane Katrina.

---

Public telecommunications networks can successfully handle a local power outage or short-term outage, such as the August 14, 2003, Northeast blackout. However, a major concern exists with outage durations that range in weeks or months. The widespread collapse of the electric grid due to an EMP event would lead to cascading effects on interdependent infrastructures, as happened during the Katrina blackout. This may well lead to a long-term loss of telecommunications in extended geographic areas outside the power loss. This loss would cascade to any critical applications that depend on telecommunications. As such, telecommunications resilience would greatly benefit from steps to increase power grid and backup power reliability and availability time frames.

Telecommunications network managers have indicated that a key asset in any outage event is the ability to monitor the health of the network in real time to enable rapid response to identified problems. Given the increased level of automation in telecommunications networks coupled with reduction in personnel, it is critical that the telecommunications operations and control functions remain operational in an EMP event. In recovering from an EMP attack, telecommunications carriers will depend on hardware and software systems that help isolate problem areas and implement commands to initiate remediation efforts. Computer servers, personal computers, routers, and related equipment are key components that are housed in Network Management Centers. Carriers typically deploy the equipment in geographically diverse centers in which one center can back up the others. Effects to those centers are moderated in cases in which the centers are separated by distances larger than the EMP footprint.

### **Recommendations**

Based on the analytical efforts performed by this Commission, the following steps are recommended to improve telecommunications performance during and after an EMP event:

- ◆ Successfully evolve critical NS/EP telecommunications services to incorporate the new technologies being embedded into telecommunications networks.
- ◆ Improve the ability of telecommunications services to function for extended periods without the availability of primary power.
- ◆ Adequately address infrastructure interdependency impacts in contingency planning.
- ◆ Identify critical applications that must survive an EMP event and address any shortfalls in telecommunications services that support these applications.

These recommendations are discussed in more detail in the next few sections.

### ***Preventing Widespread Outages from New Technology***

EMP is just one of the potential sources that would lead to stressing telecommunications networks. Understanding NS/EP service performance with respect to IP technology has benefits beyond application to EMP. This issue is in line with a U.S. government interagency Convergence Working Group (CWG) finding<sup>7</sup> that noted, “The FCC should task NRIC to assess the adequacy of interoperability testing between circuit and packet switch networks ... minimize the risk of feature interactions and the introduction of additional vulnerabilities affecting reliability, availability, and security of telecommunication services supporting NS/EP users.”

---

<sup>7</sup> Convergence Working Group’s final report, *Impact of Network Convergence on NS/EP Telecommunications: Findings and Recommendations*, February 2002.

High-profile network failures have occurred as new technologies were introduced into networks. Inadequate testing prior to widespread deployment has been highlighted as a major problem in lessons learned from past outages related to new technology introduction.<sup>8</sup> These offer an incentive for the testing of new technology supporting NS/EP services prior to widespread deployment of the technologies. The use of packet switching technology to support voice services such as GETS and WPS is at the initial point of deployment. Rigorous testing is warranted prior to major deployment. With early identification, specific system EMP vulnerabilities can be addressed prior to widespread deployment.

The following are specific steps to address technology introduction concerns:

- ◆ NCS<sup>9</sup> represents a logical organization to address these areas given its mission associated with the development and maintenance of NS/EP services. NCS should partner with other appropriate organizations to determine the effects of EMP on different types of telecommunications equipment, facilities, and operations by:
  - The testing and analysis of new technologies introduced into telecommunications networks that will support NS/EP services prior to widespread introduction into the public network. IP-related equipment should be a major near-term focus of this testing and analysis. This analysis should include examining the use of standards in terms of prevention and mitigation benefits.
  - Capturing the lessons learned from future outages associated with the expected growth of voice communications by nontraditional carriers and the tremendous growth in wireless communications. It is important that such lessons learned be captured in a systematic and fiscally prudent manner.

Historically, data captured by the Federal Communications Commission (FCC) on major outages has been extremely valuable in identifying and correcting problems as they are exhibited in deployed systems. Again, this is consistent with the EMP Commission's philosophy of preventing disastrous consequences from "cheap shot" attacks.

### ***Reducing the Effects of Power Outages on the Telecommunications Infrastructure***

In a power outage, telecommunications carriers typically depend on battery supplies that last from 4 to 8 hours and in some cases fixed and mobile generators that may have up to 72 hours of operating fuel. A key concern is the potential that major telecommunications facilities may not have primary power in the event of a long-term power outage of several weeks over a wide geographic area. Among the major concerns in such events are:

- ◆ The potential that major telecommunications facilities will not have prioritized access to fuel supplies on a long-term basis in the event of a long-term, wide-scale power outage.
- ◆ Facilities running on backup generators on a long-term basis will eventually require maintenance.

---

<sup>8</sup> AT&T (Albert Lewis) correspondence with FCC, May 13, 1998; MCI (Bradley Stillman) correspondence with FCC, December 8, 1999.

<sup>9</sup> 47 CFR Part 215 designated the Executive Agent, NCS, as the focal point within the Federal Government for all EMP technical data and studies concerning telecommunications.

These concerns proved prescient when Hurricane Katrina struck in August 2005. Katrina caused a prolonged blackout that resulted in telecommunications failures precisely because of the above concerns regarding fuel supplies and maintenance for emergency generators.

After the August 2003 Northeast blackout, recommendations were put forward by the NRIC to help address this power dependency issue. As part of lessons learned discussed in an August 27, 2003, NRIC presentation on the impact of the 2003 Northeast blackout, telecom-specific references were made to re-evaluate the Telecommunications Electric Service Priority (TESP) program: “Power management and restoral practices at the tactical level are under review by carriers—may need modifications to the TESP program to mitigate additional risks,” and “Development of TESP program for cellular networks to address priority restoration of critical cellular communications facilities is needed.”<sup>10</sup> TESP promotes (on a voluntary basis) the inclusion of critical telecommunications facilities in electric service providers’ priority restoration plans.<sup>11</sup>

Lessons learned from Katrina and the NRIC evaluation of the 2003 Northeast blackout form the underpinning for the following EMP Commission recommendations:

- ◆ Improve the ability of telecommunications to withstand the sustained loss of utility-supplied electric power:
  - Task the NCS and the North American Electric Reliability Corporation (NERC), or its successor, with providing, at a minimum, biannual status reports on the need for/adequacy of priority restoration of electric power by power utilities to selected telecommunications sites.
  - Task the Department of Energy (DOE) with exploring the adequacy of financial incentives to spur analysis of alternative powering sources that offer cost-effective and viable alternatives for telecom asset powering. For example, carriers are exploring new technologies such as fuel cells to support the powering of offices.

### ***Adequately Addressing Interdependency Impacts in Contingency Planning***

The potential impact of other interdependency effects, with a priority on NS/EP services, must be considered in any analysis of recovery planning. For example, the assumption of key personnel access to transportation to operations center sites or remote access to equipment should be addressed in contingency planning. With this in mind, the NCS would be a logical organization to address this area for critical national infrastructures. Specifically, the Commission recommends the following:

- ◆ Expand the role of the NCS within the Code of Federal Regulations (CFR) Part 215 (Federal Focal Point for EMP Information) to address infrastructure interdependencies related to NS/EP telecommunications services.

Supporting this recommendation is the need to exercise the National Response Framework to determine how well the plan addresses simultaneous degradation of multiple infrastructures. Industry personnel have suggested to the EMP Commission that a tabletop exercise considering this type of scenario would be extremely useful. Exercise results should be factored into the development of an EMP scenario to be included on the DHS list of National Planning Scenarios. Such an exercise would be invaluable in

<sup>10</sup> Aduskevicz, P., J. Condello, Capt. K. Burton, Review of Power Blackout on Telecom, NRIC, August 27, 2003, quarterly meeting.

<sup>11</sup> Homeland Security Physical Security Recommendations for Council Approval, Letter to Richard C. Notebaert, March 5, 2003.



understanding the impacts of telecommunications failures on other infrastructure sectors and vice versa. Of particular concern is the impact of losing telecommunications on the operating effectiveness of Supervisory Control and Data Acquisition (SCADA) systems for infrastructures such as electric power and natural gas.

Specifically, the Commission recommends the following:

- ◆ Task DHS with developing exercises and an additional National Planning Scenario incorporating a large-scale degradation for multiple infrastructures over a wide geographic area as might occur in an EMP event.

***Improving the Ability of Telecommunications Networks That Support Nationally Critical Applications to Survive EMP by Protecting Key Assets and Conducting Vulnerability Assessments***

The Commission recommends the following:

- ◆ Task NCS to identify key telecommunications network assets whose degradation can result in the loss of service to a large number of users. These might include next-generation routing and transport equipment and wireless network elements such as HLRs and Visiting Location Registers (VLRs). Cellular base stations should be part of this analysis.
- ◆ Task NCS through DHS, in accordance with the CFR for Telecommunications Electromagnetic Disruptive Effects (TEDE) affecting NS/EP telecommunications, to work with government and multiple industries (e.g., Federal Reserve Board and BITS [financial services], Federal Energy Regulatory Commission [FERC] and NERC [electric power], and DHS and first responders [civilian restoration]) to determine whether a high-reliability telecommunications service or services supporting mission-critical applications is needed. If so, consider partial federal funding for this service.
- ◆ Establish a reporting process to be developed by the FCC, NCS, and the telecommunications industry for reporting major outages from wireless, data communications, and Internet carriers to the FCC, analogous to what is done for wireline carriers, thereby capturing lessons learned.



## Chapter 4. Banking and Finance

### Introduction

The financial services industry comprises a network of organizations and attendant systems that process instruments of monetary value in the form of deposits, funds transfers, savings, loans, and other financial transactions. Virtually all economic activity in the United States (U.S.) and other developed countries depends on the functioning of the financial services industry. National wealth is the sum of all economic value, as reflected in part in existing capital and financial transactions. Most simply, the financial services industry is the medium and record keeper for financial transactions and repository of national, organizational, and individual wealth.

Today, most significant financial transactions are performed and recorded electronically; however, the ability to carry out these transactions is highly dependent on other elements of the national infrastructure. According to the President's National Security Telecommunications Advisory Committee (NSTAC), "The financial services industry has evolved to a point where it would be impossible to operate without the efficiencies of information technology and networks."<sup>1</sup>

The automation of the financial services industry has spurred the growth of wealth by increasing greatly the amount of business that can be conducted on a daily basis. For example, "in the early 1970s, the New York Stock Exchange [NYSE] closed every Wednesday to clear backlogs from an average daily trading volume of 11 million shares."<sup>2</sup> Today, the Securities Industry Automation Corporation (SIAC) has no interruption in exchange operations and routinely handles an average daily trading volume of more than 3 billion shares.<sup>3</sup>

"SIAC is responsible for providing the highest quality, most reliable and cost-effective systems to support the current and future business needs of the New York Stock Exchange"<sup>4</sup> and other institutions. "SIAC's Shared Data Center alone is linked to the securities industry by more than a thousand communications lines over which an average of 70 billion bytes of data is transmitted daily."<sup>5</sup> SIAC's Secure Financial Transaction Infrastructure, "improves the overall resilience of the financial industry's data communications connectivity...and offers firms reliable access to... trading, clearing and settlement, market data distribution, and other services."<sup>6</sup>

The technological revolution has not been limited to giant corporations. The individual consumer has witnessed the growth of convenient, on-demand money-dispensing

---

<sup>1</sup> United States, The President's National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report* (Washington, 1997), 4.

<sup>2</sup> Ibid.

<sup>3</sup> "Firsts and Records," NYSE Euronext, New York Stock Exchange Euronext, <http://www.nyse.com/about/history/1022221392987.html>.

<sup>4</sup> Network General Corporation, Securities Industry Automation Corporation — SIAC: Sniffer Distributed, San Jose, 2005, 1.

<sup>5</sup> Ibid.

<sup>6</sup> Boston Options Exchange, Telecom Connections, August 3, 2003, <http://www.bostonoptions.com/conn/tel.php>.

automated teller machines (ATM) in the United States from less than 14,000 in 1979<sup>7</sup> to more than 371,000 in 2003.<sup>8</sup>

The trend in the U.S. financial infrastructure is toward ever more sophisticated and powerful electronic systems capable of an ever increasing volume and velocity of business. The increasing dependence of the United States on an electronic economy, so beneficial to the management and creation of wealth, also increases U.S. vulnerability to an electromagnetic pulse (EMP) attack.

For example, the terrorist attacks of September 11, 2001, demonstrated the vulnerabilities arising from the significant interdependencies of the Nation's critical infrastructures. The attacks disrupted all critical infrastructures in New York City, including power, transportation, and telecommunications. Consequently, operations in key financial markets were interrupted, increasing liquidity risks for the U.S. financial system.<sup>9</sup>

An interagency paper jointly issued by the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), and the Securities and Exchange Commission (SEC), specifies clearing and settlement systems as the most critical business operations at risk for financial markets.<sup>10</sup> Because financial markets are highly interdependent, a wide-scale disruption of core clearing and settlement processes would have an immediate systemic effect on critical financial markets.<sup>11</sup>

Moreover, in December 2002, the FRB revised its policy and procedures for national security and emergency preparedness telecommunications programs administered by the National Communications System (NCS) to identify those functions supporting the Federal Reserve's national security mission to maintain national liquidity.<sup>12</sup> The FRB expanded the scope of services that would seriously affect continued financial operations if a telecommunications disruption of "a few minutes to one day" occurred.<sup>13</sup> These functions, which are listed below, "require same-day recovery and are critical to the operations and liquidity of banks and the stability of financial markets".<sup>14</sup>

- ◆ Large-value interbank funds transfer, securities transfer, or payment-related services
- ◆ Automated clearing house (ACH) operators
- ◆ Key clearing and settlement utilities
- ◆ Treasury automated auction and processing system

<sup>7</sup> United States, The President's National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report* (Washington, 1997), 47.

<sup>8</sup> ATM & Debit News, September 10, 2003, ATM & Debit News Survey Data Offers Insight into Debit Card and Network Trends in Its 2004 EFT Data Book, press release, <http://www.sourcemediacom/pressreleases/20030910ATM.html>.

<sup>9</sup> MacAndrews, James J., and Simon M. Potter, "Liquidity Effects of the Events of September 11, 2001," Federal Reserve Bank of New York Economic Policy Review, November 2002.

<sup>10</sup> The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (Washington: GPO, 2002), 5.

<sup>11</sup> Systemic risk includes the risk that failure of one participant in a transfer system or financial market to meet its required obligations will cause other participants to be unable to meet their obligations when due, causing significant liquidity or credit problems or threatening the stability of financial markets. The use of the term "systemic risk" in this report is based on the international definition of systemic risk in payments and settlement systems provided in Committee on Payment and Settlement Systems, Bank for International Settlements, "A Glossary of Terms in Payment and Settlement Systems," 2001.

<sup>12</sup> "Federal Reserve Board Sponsorship for Priority Telecommunications Services of Organizations That Are Important to National Security/Emergency," *Federal Register*, 67:236 (December 9, 2002), 72958.

<sup>13</sup> Ibid.

<sup>14</sup> Ibid.

- ◆ Large-dollar participants of these systems and utilities.<sup>15</sup>

The increasing dependence of the United States on an electronic economy also adds to the adverse effects that would be produced by an EMP attack. The electronic technologies that are the foundation of the financial infrastructure are potentially vulnerable to EMP. These systems are also potentially vulnerable to EMP indirectly through other critical infrastructures, such as the electric power grid and telecommunications.

### The Financial Services Industry

In a December 1997 study, *Financial Services Risk Assessment Report*, NSTAC described the financial services industry as comprising four sectors. This definition is reflected or shared in current U.S. government reports, regulations, and legislation that treat the financial services industry as having these components:

- ◆ Banks and other depository institutions
- ◆ Investment-related companies
- ◆ Industry utilities
- ◆ Third-party processors and other services.

*Banks and Other Depository Institutions.* In 2004, U.S. banks held more than \$9 trillion<sup>16</sup> of domestic financial assets, and investment companies and other private institutions held about \$17 trillion of the national wealth.<sup>17</sup> Banks and other depository institutions, including thrifts, credit unions, and savings and loan associations, are vital to the functioning of the economy. These institutions hold and provide access to deposits, provide loans, transfer funds, promote savings, and facilitate economic growth.

Commercial banks are the repository of the most financial assets of any depository institution. Commercial banks disseminate financial information, act as agents in buying and selling securities, serve as trustees for corporations or individuals, transfer funds, collect deposits, and provide credit. The top 10 commercial banks control nearly half of all assets held by banks.<sup>18</sup>

Credit unions, savings and loan associations, and savings banks generally are referred to as “other depository institutions.” These institutions usually service households instead of businesses. Credit unions are the most financially significant of these institutions. By the end of 2004, credit unions had more than 85 million members and managed more than \$668 billion in assets.<sup>19</sup>

The single most important banking institution is the Federal Reserve System. Established by the U.S. Congress in 1913, the Federal Reserve System is the central bank of the United States. This system does not deal directly with the general public, but with other banks. It is, in essence, the Nation’s bank for commercial banks.

The primary purpose of the Federal Reserve System is to maintain the stability, safety, and flexibility of the financial system and contain systemic risk that may arise in the

---

<sup>15</sup> Ibid.

<sup>16</sup> United States, Federal Reserve Board, *Federal Reserve Bulletin Statistical Supplement* (Washington: GPO, 2004), 15.

<sup>17</sup> Investment Company Institute, *2005 Investment Company Factbook*, 2005, <http://www.ici.org/factbook>.

<sup>18</sup> Klee, Elizabeth C., and Fabio M. Natalluci, “Profits and Balance Sheet Developments at U.S. Commercial Banks in 2004,” *Federal Reserve Bulletin*, Spring 2005:144.

<sup>19</sup> United States Credit Union Statistics, Credit Union National Association, 2004, [http://advice.cuna.org/download/us\\_totals.pdf](http://advice.cuna.org/download/us_totals.pdf).



financial markets. The Federal Reserve accomplishes this mission by establishing monetary policy, by servicing financial institutions and other government agencies, and by regulating and supervising banks.

As the central bank of the United States, the Federal Reserve System extends emergency credit to commercial banks and controls interest rates, foreign exchange, and the money supply. The Federal Reserve also performs check-clearing and processing and transfer of government securities and funds between financial institutions.

Federal Reserve System banks are supervised by a Board of Governors who are appointed by the president and confirmed by the U.S. Senate; however, the banks are owned by private member banks. For administrative purposes, the United States is divided into 12 Federal Reserve Districts, each district served by a Federal Reserve Bank. The 12 Federal Reserve Banks are located in New York, Boston, Philadelphia, Richmond, Atlanta, Cleveland, Chicago, St. Louis, Kansas City, Dallas, Minneapolis, and San Francisco.

*Investment-Related Companies.* Unlike commercial banks, underwriters, brokerages, and mutual funds are not depository institutions. Rather, these institutions provide a wide range of services to institutional and individual investors. They act as intermediaries in pooling investments by a large group of customers and in market trades.

Investment banks and underwriters finance investments by government and commercial enterprises through stocks and bonds. Investment banks also arrange mergers. Currently, the largest 50 firms hold 90 percent of the market share.<sup>20</sup>

Brokerages help investors by acting as agents or intermediaries with commodities and securities markets. Brokerages advise clients, perform research, and place trades. "The securities brokerage industry in the United States includes fewer than 400 companies with combined annual revenue of over \$100 billion. The top 50 companies hold over 80 percent of the market share."<sup>21</sup>

Mutual funds pool money from many people and institutions and invest it in stocks, bonds, or other securities. A portfolio manager is employed by the mutual fund to achieve its financial objective, such as providing a reliable source of investment income or maximizing long-term returns. The mutual fund market is dominated by 25 companies. The top five companies hold one-third of the market. The mutual fund industry holds about \$8.1 trillion dollars in assets.<sup>22</sup>

*Industry Utilities.* Banks, including the Federal Reserve System, and investment-related companies, such as investment banks, brokerages, and mutual funds, all rely on industry utilities to transact business. Financial service utilities are the institutions that provide a common means for transferring, clearing, and settling funds, securities, and other financial instruments, as well as exchanging financial information.

Financial industry utilities have largely replaced paper transactions with electronic means. Check and cash transactions are still the largest number of financial transactions in the national economy. However, paper transactions are vastly surpassed in total value

---

<sup>20</sup> "Industry Overview: Investment Banking," Hovers, Inc.,  
[http://www.hoovers.com/investment-banking/--ID\\_209--/free-ind-fr-profile-basic.xhtml](http://www.hoovers.com/investment-banking/--ID_209--/free-ind-fr-profile-basic.xhtml).

<sup>21</sup> Ibid.

<sup>22</sup> Investment Company Institute, *2005 Investment Company Factbook*, 2005, 59,  
[http://www.ici.org/factbook/pdf/05\\_fb\\_table01.pdf](http://www.ici.org/factbook/pdf/05_fb_table01.pdf).

by electronic transactions through wire transfers, interbank payment systems, ACHs, and clearing and settlement systems for securities and other investments.

Modern financial services utilities have transformed the national economy from a paper system into an electronic system. Examples of some key industry utilities include FEDNET, Fedwire, ACH, Clearing House Interbank Payments System (CHIPS), the Society for Worldwide Interbank Financial Telecommunications (SWIFT), the National Association of Securities Dealers' Automated Quotation System (NASDAQ), the NYSE, the New York Mercantile Exchange (NYMEX), and the Depository Trust and Clearing Corporation (DTCC).

FEDNET is a communications system connecting all 12 Federal Reserve Banks nationwide and the financial services industry generally. FEDNET transfers funds in real time among banks and other depository institutions, performs real-time sales and record keeping for the transfer of government securities, and serves as ACH.

Fedwire is the primary national network for the transfer of funds between banks; the system currently serves approximately 7,500 institutions. Fedwire's book-entry securities transfer application allows banks and other depository institutions to transfer U.S. government securities. This network has enabled the Federal Reserve to largely replace paper U.S. government securities with electronic book entries. Transfers performed on Fedwire are irrevocable upon receipt and are settled immediately. The average value of a Fedwire funds transaction is about \$3.9 million dollars.<sup>23</sup> In 2005, Fedwire processed an average daily volume of approximately 528,000 payments, with an average daily value of about \$2.1 trillion.<sup>24</sup>

ACH was developed in the 1970s as an alternative to the traditional paper-based system for clearing checks. ACH electronic transactions include direct deposits of payrolls, pensions, benefits, and dividends and direct bill payments. The Federal Reserve annually processes about 36.7 billion ACH payments valued at \$39.9 trillion dollars.<sup>25</sup>

CHIPS is an electronic system for interbank transfer and settlement. CHIPS is the primary clearing system for foreign exchange. "It processes over 285,000 payments a day with a gross value of \$1.4 trillion." This includes 95 percent of all international U.S. dollar payments.<sup>26</sup>

The SWIFT provides stock exchanges, banks, brokers, and other institutions with a cost-effective, secure international payment message system. These messages are instructions between banks and other institutions regarding payments and transfers, not payments themselves. SWIFT carries approximately 8 million messages daily.<sup>27</sup>

The NASDAQ and the NYSE are the largest securities markets. NASDAQ is an electronic communications network that consolidates the quotations of multiple dealers, displayed in real time, and allows electronic trading. The NYSE offers similar electronic

---

<sup>23</sup> Federal Reserve Board, <http://www.federalreserve.gov/paymentsystems/coreprinciples/default.htm#fn12>.

<sup>24</sup> Ibid.

<sup>25</sup> United States, Federal Reserve System, *Analysis of Noncash Payments Trends in the United States: 2000–2003* (Washington: 2004), 5.

<sup>26</sup> SWIFT, *2005 Annual Report: Alternative Connectivity for CHIPS Reinforces Resilience*, [http://www.swift.com/index.cfm?item\\_id=59677](http://www.swift.com/index.cfm?item_id=59677).

<sup>27</sup> SWIFT, *2004 Annual Report: SWIFTnet Now the Benefits Really Begin*, [http://www.swift.com/index.cfm?item\\_id=56868](http://www.swift.com/index.cfm?item_id=56868).

services. NASDAQ executed 957.9 million trades valued at more than \$3.7 trillion dollars in 2004, and the NYSE traded a slightly lesser amount.<sup>28</sup>

The NYMEX trades on futures contracts such as unleaded gasoline, heating oil, crude oil, natural gas, and platinum. NYMEX typically conducts crude oil transactions involving the total daily production of the entire world.

The DTCC settles securities trades for participant banks and is the largest securities depository in the world. In 2004, the company completed financial settlement for a quadrillion dollars in securities transactions. DTCC keeps records on securities and conducts transactions electronically. Annually, DTCC participants deliver securities valued at about \$4.5 trillion to DTCC to make electronic records of ownership.<sup>29</sup>

*Third-Party Processors and Other Services.* Third-party processing companies are technology companies that provide electronic processing services to financial institutions. Banks and other financial institutions can cut overhead by contracting with third parties to perform the mechanics of electronic transactions. Technology-related outsourcing is especially appealing because of dynamic changes in technology. The high cost and complexity of new technologies has driven many banks into partnerships with third-party specialists in the field of electronic finance. Services typically offered by third-party processors include data center management, network management, application development, check and statement processing, mutual fund account processing, and electronic funds transfer.

### **Vulnerability to EMP**

The financial infrastructure is highly dependent on electronic systems, which should be clear from the preceding discussion. Virtually all transactions involving banks and other financial institutions happen electronically. Virtually all record keeping of financial transactions are stored electronically. Just as paper money has replaced precious metals, so an electronic economy has replaced the paper one. The financial infrastructure is a network of simple and complex electronic machinery, ranging from telephones to main-frame computers, from ATMs to vast data storage systems.

The electronic technologies that are the foundation of the financial infrastructure are potentially vulnerable to EMP. These systems also are potentially vulnerable to EMP indirectly through other critical infrastructures, such as the power grid and telecommunications.

The financial services industry and knowledgeable experts on the security of that industry judge that the industry is highly robust against a wide range of threats. The NSTAC, for example, notes that the leading financial institutions take a multilayered approach to building robustness and recoverability into their systems:

*Operational data centers are engineered from the ground up with survivability in mind. Some are hardened with thick concrete walls and protected with extensive perimeter security measures equivalent to military command posts. Most have uninterruptible power supplies, generators, and on-site fuel*

<sup>28</sup> NASDAQ, *NASDAQ Announces Market Year-end Statistics for 2004*, <http://ir.nasdaq.com/releasedetail.cfm?ReleaseID=177077>.

<sup>29</sup> DTCC, *2004 Annual Report: What is a Quadrillion?* 3, [http://www.dtcc.com/downloads/annuals/2004/2004\\_report.pdf](http://www.dtcc.com/downloads/annuals/2004/2004_report.pdf).

*storage sufficient to allow the facility to run independently of the power grid ranging from a few hours to over a month. External telecommunications links are diversely homed, with multiple building access points and connections to more than one central office...wherever possible. Operational procedures within the data center are designed to minimize the risk of human errors causing interruptions, and most or all data files are copied and stored on disk or tape at off-site facilities.*<sup>30</sup>

NSTAC also observes that, “Numerous natural and man-made disasters...have forced financial institutions to test and refine their disaster recovery capabilities.”<sup>31</sup> The financial services industry’s dependence on other infrastructures has been tested in real emergencies. For example, in 1988, a fire in the Ameritech central office in Hinsdale, Illinois, disabled long-distance telecommunications for the Chicago Board of Trade and other major institutions. Wall Street was blacked out for nearly a week by an electrical fire in a Consolidated Edison office in August 1990. In April 1992, underground flooding in Chicago caused sustained telecommunication and power outages. Financial institutions faced widespread electrical power outages in the West during the summer of 1996 and in the Northeast during the summer of 2003.

“In addition,” according to NSTAC, “the industry weathered one of the worst terrorist attacks in recent history”:

*The World Trade Center bombing on February 26, 1993, struck at the industry’s heart, affecting the New York Mercantile Exchange and many securities dealers and otherwise disrupting activities throughout Wall Street. Numerous problems with facilities, systems, procedures, and staffs were encountered as firms scurried to recover, and some securities firms’ operations were shut down temporarily. However, none of the most critical services were affected, and the effect on the economy as a whole was minimal.*<sup>32</sup>

The financial services industry also weathered the more devastating terrorist attack on September 11, 2001, that destroyed the World Trade Center. NSTAC found that these types of events, “led to improved robustness of the financial services infrastructure.”

NSTAC’s judgment that the financial services industry enjoys robust survivability against a wide range of threats is seconded by the National Academy of Sciences (NAS) in its study, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (2002). According to the NAS, the U.S. financial infrastructure is highly secure because of the redundancy of its electronic systems: “While no law of physics prevents the simultaneous destruction of all data backups and backup facilities in all locations, such an attack would be highly complex and difficult to execute, and is thus implausible.”<sup>33</sup>

<sup>30</sup> United States, The President’s National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report* (Washington, 1997), 40.

<sup>31</sup> Ibid.

<sup>32</sup> Ibid.

<sup>33</sup> National Academies of Science, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington: National Academies Press, 2002), 137.

However, the NSTAC and NAS studies were focused primarily on the threat to the financial services industry from cyberterrorists using computer-based attacks. These studies did not evaluate the threat from EMP attack.

An EMP attack would pose the very kind of simultaneous and widespread threat postulated by the NAS that would be fatal to the financial infrastructure but judged by them to be too difficult to execute and implausible for cyberterrorists. EMP effects propagate at the speed of light and would cover a broad geographic area. Such an attack potentially could achieve the NAS criteria for financial infrastructure catastrophe: "simultaneous destruction of all data backups and backup facilities in all locations."<sup>34</sup>

An EMP would probably not erase data stored on magnetic tape. However, by shutting down power grids and damaging or disrupting data retrieval systems, EMP could deny access to essential records stored on tapes and compact discs (CD). Moreover, because EMP physically destroys electronic systems, it is also in the category of threats that NSTAC concludes are more worrisome than cyberterrorism: "Physical attacks remain the larger risk for the industry."

The vast majority of electronic systems supporting the financial infrastructure have never been tested, let alone hardened, against EMP. Yet the enormous volume, speed, and accuracy required of the electronic infrastructure supporting the financial services industry allow little or no room for error. Financial operations could not tolerate the kind of disruptions or mass systemic destruction likely to follow an EMP attack.

For example, CHIPS interbank transactions typically involve about \$1.4 trillion dollars of business every day, or some \$182 billion dollars every hour.<sup>35</sup> CHIPS and Fedwire routinely receive 5 to 10 funds transfer messages each second during peak traffic periods.<sup>36</sup> The Options Clearing Corporation manages \$1.05 billion in average daily premium settlements.<sup>37</sup> On Christmas Eve 2004, a single credit card association processed over 5,000 transactions per second.<sup>38</sup> Financial institutions also must store tremendous amounts of data. Terabyte portfolios (containing 1 trillion bytes) are now common, and some databases exceed a petabyte (1,000 trillion bytes). Changes in these huge databases must be recorded at the end of every business day.

"Dealing with this kind of volume, industry utilities cannot afford any interruption in service," according to NSTAC. An EMP attack, with its potential to disrupt communications possibly for days, weeks, or months and to destroy or change databases, would place the financial infrastructure at risk.

Although the financial services industry has survived and learned from natural and man-made disasters, those disasters also have exposed vulnerabilities that could be exploited by an EMP attack. According to the staff director for management of the FRB, the terrorist attack of September 11, 2001, on the World Trade Center exposed telecommunications and the concentration of key facilities as serious weaknesses of the financial

<sup>34</sup> Ibid.

<sup>35</sup> SWIFT, 2005 Annual Report: Alternative Connectivity for CHIPS Reinforces Resilience, [http://www.swift.com/index.cfm?item\\_id=59677](http://www.swift.com/index.cfm?item_id=59677).

<sup>36</sup> Ibid.

<sup>37</sup> One Chicago (April 30, 2002), ONECHICAGO, Options Clearing Corporation and Chicago Mercantile Exchange, Inc., Sign Clearinghouse Agreements, press release, [http://www.onechicago.com/060000\\_press\\_news/press\\_news\\_2002/04302002.html](http://www.onechicago.com/060000_press_news/press_news_2002/04302002.html).

<sup>38</sup> "Digital Transactions News," *Digital Transactions*, January 6, 2005, MasterCard Worldwide, Digital Transactions, <http://www.digitaltransactions.net/newsstory.cfm?newsid=466>.



services industry. Equity markets closed for 4 days, until September 15, due to failed telecommunications. The NYSE could not reopen because key central offices were destroyed or damaged, leaving them unable to support operations. According to this senior government official, Fedwire, CHIPS, and SWIFT would cease operation if telecommunications were disrupted. He further observed that ACH, ATMs, and credit and debit cards all depend on telecommunications. Disruption of these systems would force consumers to revert to a cash economy.<sup>39</sup>

Further, response to the Northeast power outage in August 2003 has been depicted as a triumph for the financial services industry safeguards implemented since the terrorist attacks of September 11, 2001. But this is not the whole picture. Some analysts observe that the blackout happened under nearly ideal conditions to facilitate financial industry recovery. The blackout happened on a Thursday at 4:10 p.m., after the 4:00 p.m. closing time for financial markets, and it was largely over for the financial industry by 9:00 a.m. the following Friday morning. Business was also light, at its nadir, as is usual during August.

Even so, recovery from the 2003 blackout still required many in the financial industry to work overnight. The American Stock Exchange did not open because its air conditioners would not operate. Many traders could not get to work on Friday because the transportation system was paralyzed. Some companies were unable to reach the NASDAQ electronic exchange by telephone. Many ATMs failed. Many of the 1,667 banks in New York City closed on Friday because of continuing power outage. Many industries with back-up generators, like KeyCorp in Cleveland, were unprepared for a blackout that lasted for more than a few hours, and they had difficulty getting diesel fuel.

The fortunate timing and short duration of the 2003 blackout affected the financial industry for a relatively brief period. Nonetheless, banks had to compensate for financial imbalances by borrowing \$785 million dollars from the Federal Reserve System. This was 100 times the amount borrowed the previous week, and the greatest amount borrowed since the week after the September 11 attacks.<sup>40</sup> Most economists concur that the blackout had a small but measurable effect on the U.S. third-quarter economic growth.

These observations suggest that, if an EMP attack were to disrupt the financial industry for days, weeks, or months rather than hours, the economic impact would be catastrophic. The prolonged blackout resulting from Hurricane Katrina in August 2005 is a far better example than the Northeast blackout of 2003 of the challenge that would be posed to the financial infrastructure from EMP. The Katrina blackout, comparable to a small EMP attack, disrupted normal business life for months and resulted in a staggering economic loss that is still an enormous drain on the national economy.

The financial network is highly dependent on power and telecommunications for normal operations. Widespread power outages would shut down the network, and all financial activity would cease until power was restored, as happened during Hurricane Katrina. Even if power were unaffected or restored in short order, full telecommunications are required to fully enable the financial network. If critical elements within the telecommunications infrastructure were negatively affected by the EMP attack (i.e., at main and

<sup>39</sup> Malphrus, Steve, Staff Director for Management, Federal Reserve Board, personal communication.

<sup>40</sup> Jackson, William D., *Homeland Security: Banking and Financial Infrastructure Continuity*, U.S. Congress, March 16, 2004, Congressional Research Service (Washington, 2004), 6, <http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL3187303162004.pdf>.

local switches), the financial network would be impacted negatively to some degree and consequently be highly dependent on the telecommunication recovery timelines before it could be brought back online with the required capability and capacity.

The extent to which the financial network is able to function as it is being brought back online will be highly dependent on the level of damage incurred by the network as a result of the EMP attack.

### **Consequences of Financial Infrastructure Failure**

Despite the robustness of U.S. financial infrastructures against a wide range of threats, they were not designed to withstand an EMP attack. Indeed, the highly sophisticated electronic technologies that make the modern U.S. financial infrastructure possible are the components most vulnerable to EMP.

An EMP attack that disrupts the financial services industry would, in effect, stop the operation of the U.S. economy. Business transactions that create wealth and jobs could not be performed. Loans for corporate capitalization and for private purposes, such as buying homes and automobiles could not be made. Wealth, recorded electronically in bank databases, could become inaccessible overnight. Credit, debit, and ATM cards would be useless. Even reversion to a cash economy might be difficult in the absence of electronic records that are the basis of cash withdrawals from banks. Most people keep their wealth in banks and have little cash on hand at home. The alternative to a disrupted electronic economy may not be reversion to a 19th century cash economy, but reversion to an earlier economy based on barter.

In the immediate aftermath of an EMP attack, banks would find it very difficult to operate and provide the public with the liquidity they require to survive; that is, to buy food, water, gas, or other essential supplies and services. Modern banking depends almost entirely on electronic data storage and retrieval systems for record keeping and to perform account transactions. An EMP attack that damages the power grid or electronic data retrieval systems would render banking transactions virtually impossible as a practical or legal matter.

Operating a banking system using paper and handwritten transactions would be difficult without access to the information contained in electronic records. If a makeshift paper banking system could be organized on an emergency basis, such a system would be fraught with the risk of fraud, theft, and costly mistakes. Such a system would not be consistent with the cautious behavior and natural interest of banks in assigning highest priority to protecting financial assets. Protocols and business standards that are required of banks under their charters for insurance purposes and to protect them from legal liability assume the existence of modern electronic banking systems and the reliability, redundancy, and surety that such systems provide.

A survey by Commission staff of natural and man-made disasters found no case in which banks, bereft of their electronic systems because of blackout, reopened their doors and did business by hand. Unless banks have well-prepared contingency plans in place to revert to paper and handwritten transactions in advance of a crisis, it is very doubtful that bank managers would have the capability, authority, or motivation to attempt a paper and handwritten banking system in the aftermath of an EMP attack. Unless directed by federal authority to create contingency plans for operating without electricity, it is doubtful the business community would undertake such plans on its own.

In the aftermath of an EMP attack, individuals and corporations would have many sound reasons for being cautious, risk averse, and unwilling to resume business as usual. Once power, telecommunications, and transportation are restored, even if restored promptly, within a matter of days, psychological concerns that affect economic revitalization may linger. Full recovery will require restoring the trust and confidence of the business community in the infrastructures, in financial institutions, and in the future. The Great Depression outlasted its proximate causes by many years, despite strenuous efforts by the Federal Government to implement financial reforms and jump-start the economy, in part because businesses were unwilling to risk their capital in a system that had lost their confidence.

The Department of the Treasury and the SEC share the view that failure of electronic systems supporting the critical infrastructure for even one business day threatens the financial system with wide-scale disruption and risk to one or more critical markets. Indeed, the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, by the Department of the Treasury and the SEC advocates “the overall goal of achieving recovery and resumption within two hours after an event.” It states:

*In light of the large volume and value of transactions/payments that are cleared and settled on a daily basis, failure to complete the clearing and settlement of pending transactions within the business day could create systemic liquidity dislocations, as well as exacerbate credit and market risk for critical markets. Therefore, core clearing and settlement organizations should develop the capacity to recover and resume clearing and settlement activities within the business day on which the disruption occurs with the overall goal of achieving recovery and resumption within two hours after an event.*<sup>41</sup>

Partial or small-scale disruption of the financial infrastructure would probably be enough to bring about a major economic crisis. Nonfunctioning ATM machines, for example, and other impediments to obtaining cash might well undermine consumer confidence in the banking system and cause a panic. NSTAC observes that the ultimate purpose behind all the financial industry’s security efforts is to retain consumer confidence: “The ability of an institution to maintain the trust, and hence, the business, of its customers is viewed as an even greater value than the dollars and cents involved.”<sup>42</sup> A related NAS study concludes that an attack that destroys only electronic records would be “catastrophic and irreversible.”<sup>43</sup> Although it is highly unlikely that stored financial data on magnetic media would be damaged by EMP, the electronic systems for retrieving data are potentially vulnerable to EMP and are dependent on a vulnerable power grid. Data and essential records are useless if inaccessible. According to the NAS, “Irrecoverable

<sup>41</sup> U.S. Security Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, April, 2003.

<sup>42</sup> United States, The President’s National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report* (Washington, 1997), 27.

<sup>43</sup> National Academies of Science, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington: National Academies Press, 2002), 137.

loss of critical operating data and essential records on a large scale would likely result in catastrophic and irreversible damage to U.S. society.”<sup>44</sup>

### Recommendations

Securing the financial services industry from the EMP threat and from other threats is vital to the national security of the United States. The Federal Government must ensure that this system can survive sufficiently to preclude serious, long-term consequences.

The Department of Homeland Security, the FRB, and the Department of the Treasury, in cooperation with other relevant agencies, must develop contingency plans to survive and recover key financial systems promptly from an EMP attack.

Key financial services include the means and resources that provide the general population with cash, credit, and other liquidity required to buy essential goods and services. It is essential to protect the Nation’s financial networks, banking records, and data retrieval systems that support cash, check, credit, debit, and other transactions through judicious balance of hardening, redundancy, and contingency plans.

The Federal Government must work with the private sector to ensure the protection and effective recovery of essential financial records and services infrastructure systems from all deliberate adverse events, including EMP attack. Implementation of the recommendations made by the Department of the Treasury, the FRB, and the SEC in their *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* to meet sabotage and cyberthreats that could engender requirements for protection and recovery should be expanded to include expeditious recovery from EMP attack as follows:

- ◆ “Every organization in the financial services industry should identify all clearing and settlement activities in each critical financial market in which it is a core clearing and settlement organization or plays a significant role” that could be threatened by EMP attack.
- ◆ Industry should “determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets” following an EMP attack.
- ◆ Industry should be prepared to cope with an EMP attack by maintaining “sufficient geographically dispersed resources to meet recovery and resumption objectives.... Back-up sites should not rely on the same infrastructure components (e.g., transportation, telecommunications, water supply, electric power) used by the primary site. Moreover, the operation of such sites should not be impaired by a wide-scale evacuation at or inaccessibility of staff that service the primary site.”
- ◆ Industry should “routinely use or test recovery and resumption arrangements.... It is critical for firms to test back-up facilities of markets, core clearing and settlement organizations, and third-party service providers to ensure connectivity, capacity, and the integrity of data transmission” against an EMP attack.<sup>45</sup>

---

<sup>44</sup> Ibid.

<sup>45</sup> U.S. Security Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, April 2003.

## Chapter 5. Petroleum and Natural Gas

### Introduction

The United States economy is dependent on the availability of energy. While much of that energy originates in natural resources of coal, hydroelectric, and nuclear materials and is distributed to users through the electric power grid, more than 60 percent of all U.S. domestic energy<sup>1</sup> usage derives from petroleum (about 40 percent) and natural gas (more than 20 percent) and is distributed to users through an extensive national pipeline system. Refined petroleum products and natural gas power our cars, heat our homes, energize our factories, and comprise critical elements of industrial materials ranging from fertilizers to plastics, all enabling the normal functioning of our energy intensive civil society. In 2006, according to the Annual Energy Review, the United States imported an average of 10 million barrels of crude oil and 11.5 billion cubic feet of natural gas every day. Domestically the United States produced about 5 million barrels of crude and 50.6 billion cubic feet of dry gas daily. All of these energy resources were delivered from their points of production or ports of entry to users or further distribution points through the national pipeline system.

While the closely related petroleum and natural gas infrastructures comprise a variety of production, processing, storage, and delivery elements, as described in the next section, the focus of this chapter will be on the delivery system. In particular, we shall focus on the potential electromagnetic pulse (EMP) vulnerability of the more than 180,000 miles of interstate natural gas pipelines and the more than 55,000 miles of large — 8-inch to 24-inch diameter — oil pipelines.<sup>2</sup> We shall point to the potential vulnerabilities of the electronic control systems — supervisory control and data acquisition systems (SCADA) — that were discussed in general terms in Chapter 1, but whose criticality and centrality for the operation of the petroleum and natural gas infrastructure distribution systems are particularly prominent. Control system components with low voltage and current requirements, such as integrated circuits, digital computers, and digital circuitry, are ubiquitous in the U.S. commercial petroleum and natural gas infrastructures, and EMP-caused failures can induce dangerous system malfunctions resulting in fires or explosions.

### Infrastructure Description

#### Petroleum

The petroleum infrastructure can be divided into two parts: the upstream sector, which includes exploration and production of crude oil, and the downstream sector, which comprises the refining, transmission, and distribution of the finished petroleum product.

Physical components of the upstream sector include land oil wells and waterborne oil rigs for exploration, drilling, and extraction of crude oil. In 2006, there were 274 rotary rigs operating on- and off-shore in the United States and 501,000 crude oil producing wells (**figure 5-1**). In addition, many elements of the production of crude oil are located abroad, because the majority of U.S. oil is imported.

In contrast to the production stages of petroleum, the United States is the largest producer of refined petroleum products in the world. In 2006, 149 refineries were producing

---

<sup>1</sup> Annual Energy Review 2006, International Energy Agency.

<sup>2</sup> Pipeline 101, <http://www.pipeline101.com>.



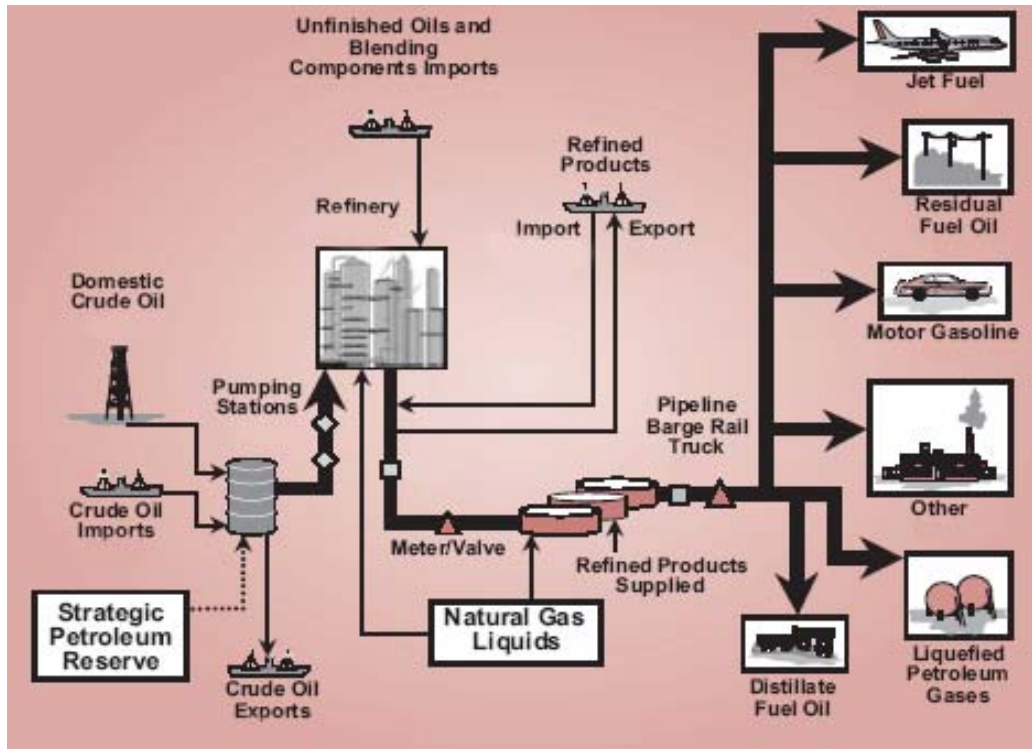


Figure 5-1. Petroleum Infrastructure<sup>3</sup>

approximately 23 percent of the world's refinery output. These refineries range in production capabilities from 5,000 barrels to approximately 500,000 barrels per day. Nearly one-half of America's refining capacity is located along the Gulf Coast, mostly in Texas and Louisiana. Other major refineries are found throughout the Midwest and in California, Washington, and along the East Coast of the United States.

The most pervasive physical element of the oil infrastructure is the extensive transmission network that moves crude oil from the field to the refineries for processing and brings the finished products to the consumer. Pipelines are the safest and most economical way to accomplish this and account for nearly 50 percent of all crude oil received in domestic refineries in 2006. Tankers transport an additional 46 percent of the crude oil received by refineries, with the remaining crude oil delivered to refineries by barge, rail tank car, and truck. There are approximately 55,000 miles of crude oil trunk lines (8-inch to 24-inch diameter) and an additional 30,000 to 40,000 miles of smaller gathering lines (2-inch to 6-inch diameter) across the United States. The trunk lines connect regional markets, while the smaller gathering lines transport crude oil from the well — on- or off-shore — to larger trunk lines and are located mainly in Texas and Louisiana. Movement of the refined products, such as gasoline, diesel, and jet fuel, to the marketplace is done largely by tankers. In addition, there are approximately 95,000 refined product pipelines nationwide, varying in diameter from 8 to 12 inches to 42 inches, that bring products to their final destinations.

Storage facilities are an integral part of the movement of oil by rail, highway, pipeline, barge, and tanker and can be aboveground, underground, or offshore. In the United

<sup>3</sup> National Petroleum Council, *Securing Oil and Natural Gas Infrastructures in the New Economy*, a Federal Advisory Committee to the Secretary of Energy, June 2001.

States, the most common storage tank is aboveground and made of steel plates. Most underground storage tanks are made out of steel as well. These storage facilities are located at each node in the production and distribution of petroleum and include tanks at the production field, marine terminals, refineries, pipeline pumping stations, retail facilities, car gasoline tanks, and home heating tanks.

In 2006, the United States imported about 60 percent of its petroleum consumption from abroad. Four thousand U.S. off-shore platforms, 2,000 petroleum terminals, and 4,000 oil tankers belonging to the world's energy trading nations and unloading petroleum at 185 ports in the United States, must also be counted as part of the petroleum infrastructure.

### **Natural Gas**

The natural gas infrastructure comprises production wells, processing stations, storage facilities, and the national pipeline system (see **figure 5-2**).

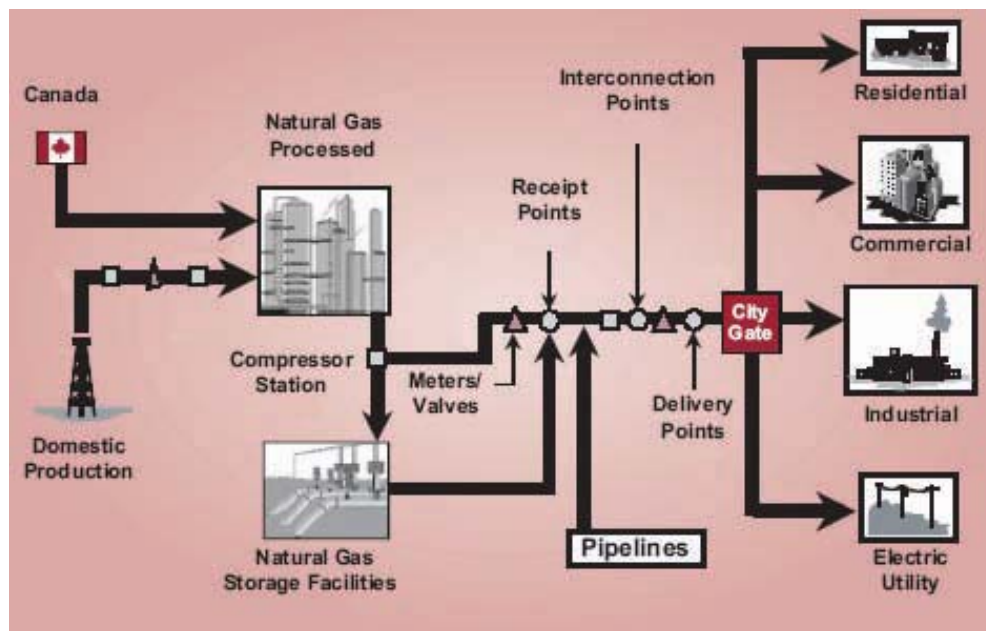


Figure 5-2. Natural Gas Infrastructure

In 2006, there were 448,461 gas- and condensate-producing wells<sup>4</sup> distributed among 63,353<sup>5</sup> oil and gas fields in the United States. There were more than 500 natural gas processing plants<sup>6</sup> and more than 1,400 compressor stations that maintain pressures in the pipeline and assure the forward motion of the transmitted gas supply. Storage facilities included 394 active underground storage fields, consisting of depleted oil and gas fields, aquifers, and salt caverns, five liquefied natural gas (LNG) import facilities, and 100 LNG peaking facilities. The pipeline system consists of more than 300,000 miles of interstate and intrastate transmission lines and an additional 1.8 million miles of smaller distribution lines that move gas closer to cities and to individual homes and business.

<sup>4</sup> Energy Information Administration, About Natural Gas, [http://www.eia.doe.gov/pub/oil\\_gas/natural\\_gas/analysis\\_publications/ngpipeline/transsys\\_design.html](http://www.eia.doe.gov/pub/oil_gas/natural_gas/analysis_publications/ngpipeline/transsys_design.html).

<sup>5</sup> Energy Information Administration, Oil and Gas Code Field Master List, 2006.

<sup>6</sup> Natural Gas Processing Plants, 1995-2004 EIA 6/2006.

Most of the natural gas consumed in the United States is produced domestically. Historically domestic production has accounted for around 85 percent of U.S. consumption with imports from Canada making up the remaining 15 percent. In recent years, domestic production has fallen to about 75 percent of consumption with the remainder imported from Canada. In 2005, five states — Texas, Oklahoma, Wyoming, Louisiana, and New Mexico — accounted for 77 percent of domestic natural gas production.

### **Direct Effects of EMP on Petroleum and Natural Gas Infrastructure**

The infrastructure described in the previous section is dependent on the continuous operation of a wide variety of electrical components: pumps to extract fuel from wells and manage its movement through pipelines, electrically driven systems to process materials in refineries, transportation systems to deliver fuels to users from storage sites, point-of-sale electronics to process transactions to retail customers, and so on — all of which represent potential points of vulnerability to an EMP pulse. We shall focus here on the vulnerability due to only one of these components — SCADA — because they represent a ubiquitous presence across all the different infrastructure elements and play a series of critical roles whose loss would severely compromise, or in some instances eliminate altogether, the ability of the infrastructure to function.

SCADA systems themselves, and their tested vulnerability to electromagnetic pulses, were described in some detail in Chapter 1, the introductory chapter to this volume, and we shall not repeat that here. Instead we describe the particular role of SCADAs within the petroleum and natural gas infrastructure, and then consider the consequences of an event which degrades or destroys the control and monitoring functions performed by the SCADAs.

### **Petroleum Infrastructure and SCADA**

SCADAs play a critical role at every stage of the oil industry's life cycle: production, refining, transportation, and distribution. Automation within the oil industry begins at the resource exploration stage and ends with final delivery to the customer. At each step, process control and SCADA are used not only to ensure that operations are efficient, but also that strict safety measures are maintained to prevent injuries and fatalities, fires and explosions, and ecological disasters.

SCADA systems, for example, are deployed in production fields, pipeline gathering systems, and along pipelines to monitor and adjust various operating parameters. These monitoring functions assist oil companies in preventing leaks and other hazardous conditions, as well as minimizing the impact of those that do occur.

These systems, which involve two-way traffic requiring paired channels, allow a master station to monitor and control the status of a multitude of measurements and tolerance limits at wellheads, pump stations, and valves, thus eliminating the need for constant manual surveillance. **Figure 5-3** presents a typical SCADA system for offshore oil production and onshore oil distribution, showing the use of remote terminal units (RTUs) and distributed control systems (DCS) at remote locations and their connection with the master terminal units (MTUs) through various communication media.

Pumping facilities that produce thousands of horsepower of energy and metering facilities that measure thousands of barrels per hour are routinely operated remotely via these SCADA systems. They can be properly operated only by using extremely reliable communications systems. The control aspect may include controls to a well pump to increase

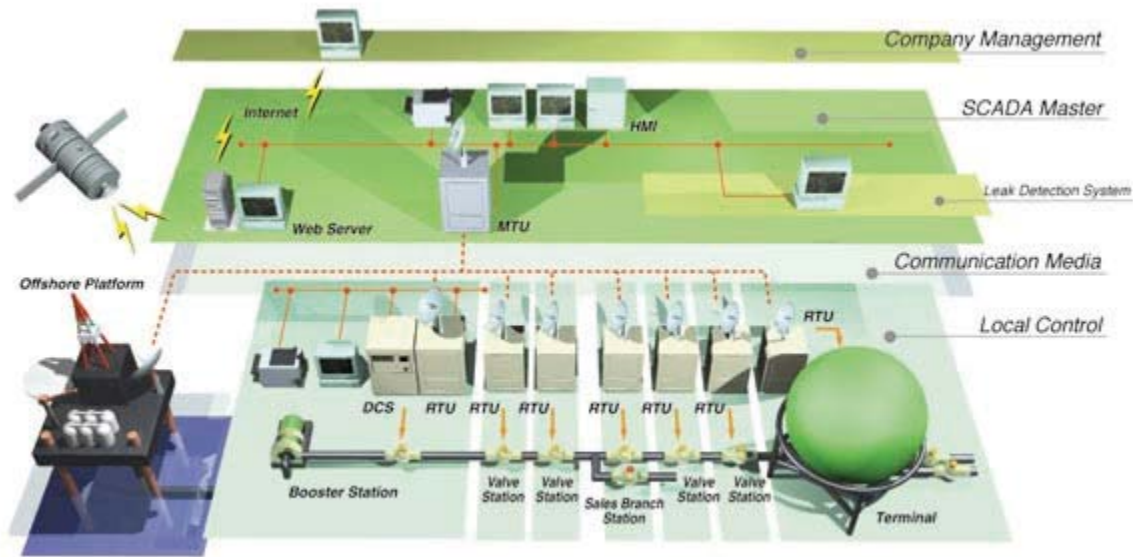


Figure 5-3. Typical SCADA Arrangement for Oil Operations

or decrease output or to shut down altogether. Pipeline controls may include changing routing, increasing or reducing the flow of the liquids or gases, and other functions. However, some pipeline facilities still require manual operation.

Process control is concerned with maintaining process variables, temperatures, pressures, flows, compositions, and the like at some desired operating value. Process control systems within refineries, along pipelines, and in producing fields were previously closed and proprietary. These control processes are now moving toward open architecture and commercially available software. The oil infrastructure now relies on e-commerce, commodity trading, business-to-business systems, electronic bulletin boards, computer networks, and other critical business systems to operate and connect the infrastructure. These assessment and control tools depend to a large degree on telecommunications and associated information technologies. Telecommunication in this context refers to a system of information linkages and data exchanges that include SCADA, the associated SCADA communication links, control systems, and integrated management information systems.

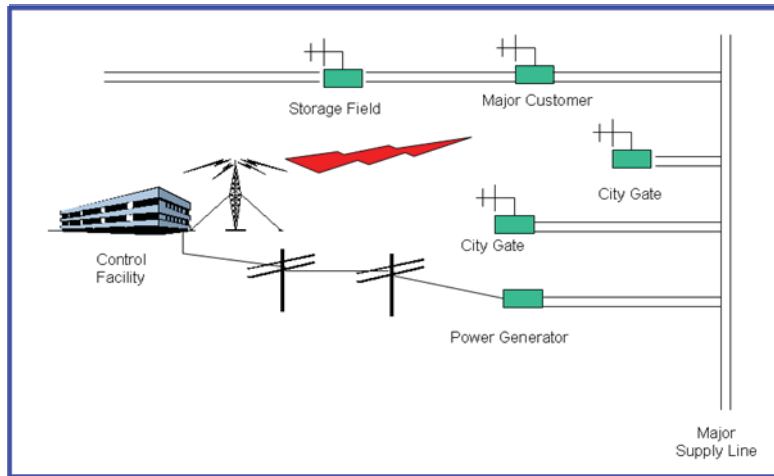
### Natural Gas Infrastructure and SCADA

SCADA is essential to modern natural gas operations. These systems provide the near-real-time data flows needed to operate efficiently in a deregulated environment. In addition, SCADA provides reporting of all transactions, establishing financial audit trails.

The key to effectively managing natural gas deliveries to customers is knowing what is happening along an interstate or intrastate pipeline system at all times. This is accomplished with Gas Control — a centralized command post that continuously receives information from facilities along the pipeline and disseminates information and operational orders to equipment and personnel in the field (see **figure 5-4**).

Through the use of SCADA equipment, Gas Control monitors volumes, pressures, and temperatures, as well as the operating status of pipeline facilities. Using microwave, telephone, or communication satellites, SCADA provides the Gas Control operator with information on the volume of natural gas flowing into the system and the volume of gas





**Figure 5-4. SCADA Integrates Control of Remote Natural Gas Facilities**

delivered to customers and gives the ability to quickly identify and react to equipment malfunctions or incidents. SCADA also gives Gas Control the capability to remotely start or stop compressors or open or close valves, thereby varying flow volumes to meet changes in customer demand for natural gas. Before the advent of SCADAs, all such functions, including tedious flow computations, were performed manually.

Automation of natural gas operations employs electronic components and technology to a high degree. Many of these components use simple mechanical or electrical properties to perform their defined roles, but an increasing number of them are computer-based. The major components and subsystems are RTUs, programmable logic controllers (PLC), MTUs, and communication systems, both wired and wireless. The total SCADA structure also includes control centers, information technology, personal computers (PC), and other peripheral technologies. RTUs and PLCs are usually located at the remote operational sites and connected to the MTUs and communication infrastructure through the communications network.

### **Effects of an EMP Event on the U.S. Petroleum and Natural Gas Infrastructures**

There are few empirical data to support definitive statements regarding the precise effects of an EMP event, should one occur. We can only extrapolate from what is known about the effects of various levels of EMP testing and what is indicated by other types of ongoing tests. It is evident that electronic devices, particularly those incorporating solid-state circuitry are, to varying degrees, susceptible to the effects of an EMP event.

The principal electronic components of a SCADA system, those devices most vulnerable to an EMP attack, are found in all the major subsystems of the SCADA installation. The MTU is a modern computer, with various solid-state circuits embedded on the microchips contained inside. An EMP event may affect these, either as a temporary disruption, which, if not automatically rebooted, might require manual intervention, or with permanent damage. If MTUs are not physically damaged, it may not be obvious whether their functional state has altered. As discussed earlier, loss of the MTU would blind the Control Center personnel to system data and performance. The physical system (e.g., pipelines, refineries) would continue to operate within the limits of the preprogrammed RTU controls, assuming that these components also have not been adversely affected by the EMP event.



The RTUs and PLCs used in today's SCADA systems rely on solid-state circuits to maintain their programming and to carry out the directives issued through those programs. This design makes the RTU and PLC inherently vulnerable to an EMP event. Although small, remote installations potentially have less exposure, it can be assumed that some or all of the RTUs and PLCs would be affected by an EMP event. As in the case of the MTU, affected embedded, integrated chips are suspect, even if the damage is not total and perhaps not immediately evident.

### **Gas**

Functional loss of the RTU and PLC results in loss of supervisory control at that location. The equipment is unable to direct changes in pressure to match changes in demand requirements for the natural gas sector. The gas delivery system should continue to operate, and natural gas should continue to flow, but ultimately the system may reach extreme conditions. Due to the presence of backup emergency pressure regulation, it is unlikely that such a failure would lead to an unsafe condition, one that would cause a rupture or explosion. The most likely result, given no manual intervention, would be significant loss of pressure after some period of time, leading to massive service disruption.

Currently, if any component of the control system (e.g., RTU, PLC, MTU) for the natural gas infrastructure fails, the system still has the mechanical ability to operate as it did in the days before SCADA. An EMP-induced false signal might affect operation if the signal unexpectedly closed a valve instead of keeping it open. The SCADA system would then have no ability to adjust to changing conditions; however, except in extreme cases such as peak winter demand conditions, it should be able to maintain deliveries until field personnel arrive and institute manual control. Discussions with natural gas system operators provide a consensus that it would be highly unlikely that the natural gas pipeline system would be shut down immediately if it is recognized that there is problem with the field data.

### **Oil**

If the SCADA system for an oil pipeline is inoperative due to the effects of an EMP event, it is the opinion of a number of former pipeline personnel that operations would have to be shut down. A petroleum pipeline failure can be catastrophic. Leaking oil could contaminate water supplies and cause disastrous fires. Based on their experience, it has been stated that companies that operate any type of complex pipeline system today do not have enough personnel to manually operate the system using on-site operators with telephone communications (which may not be available after an EMP event) to a central control center, due in part to the multiple sites that need to be monitored and controlled during an emergency. Over the past decade, there has been a trend to increase remote control capability while reducing personnel in the oil and natural gas pipeline industry.

U.S. refineries are critically dependent on the computers and integrated circuitry associated with process control, which are vulnerable to EMP effects. Discussions with plant managers and process control engineers at a number of refineries gave a nearly unanimous response that loss of process control would lead to refinery shutdown. A number of refineries stated they maintain an emergency override fail-safe system that institutes a controlled shutdown of the refinery if various SCADA parameters are out of range. However, the very short notice of a process control outage and the emergency shutdown procedure a refinery must undergo significantly increase the potential for equipment damage and lost production.

### Indirect Effects of EMP: Accounting for Infrastructure Interdependencies

Infrastructure interdependency was discussed from a more general perspective in Chapter 1. The petroleum and natural gas infrastructures provide illustrative examples of such interdependencies as illustrated in **figures 5-5** and **5-6**.<sup>7</sup>

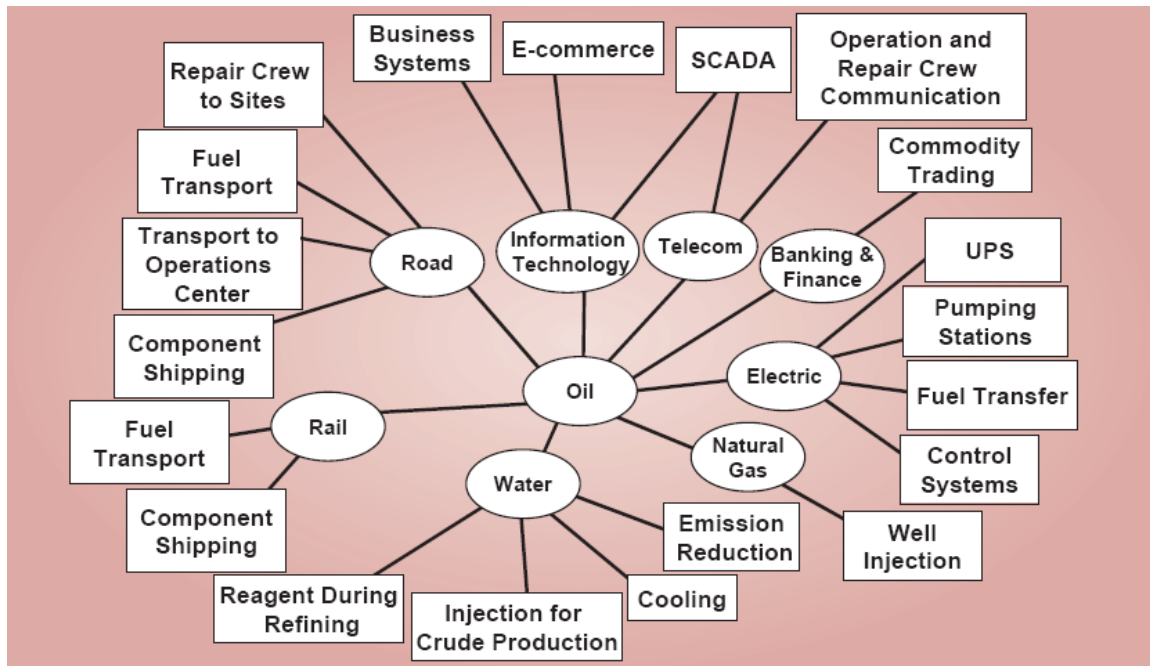


Figure 5-5. Examples of Oil Interdependencies

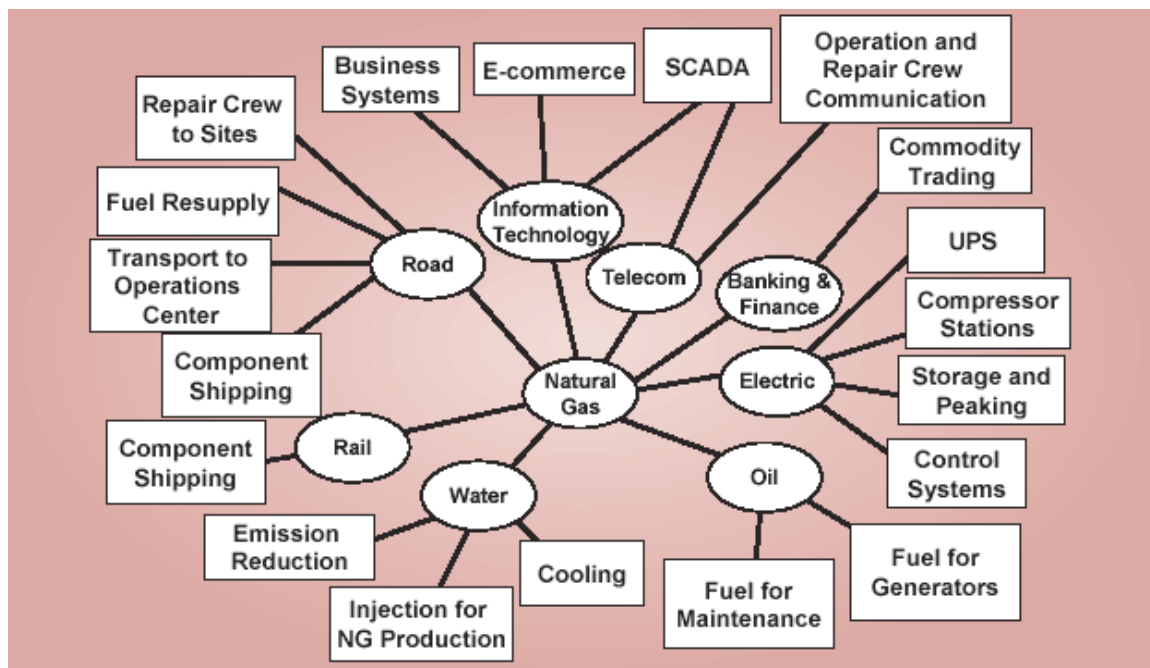


Figure 5-6. Examples of Natural Gas Interdependencies

<sup>7</sup> National Petroleum Council, Securing Oil and Natural Gas Infrastructures in the New Economy. Not all interdependencies are shown.

The petroleum and natural gas infrastructures are critically dependent on the availability of assured electric power from the national grid, as well as all the other critical national infrastructures, including food and emergency services that sustain the personnel manning these infrastructures. In turn, all these infrastructures rely on the availability of fuels provided by the petroleum and natural gas sector.

Petroleum and natural gas systems are heavily dependent on commercial electricity during the entire cycle of production, refining, processing, transport, and delivery to the ultimate consumer. The availability of commercial power is the most important dependency for the domestic oil sector. The natural gas infrastructure depends on electric power to operate lube pumps for compressors, after-cooler fans, electronic control panels, voice and data telecommunication, computers, SCADA communication and controls infrastructure, gas control centers, and other critical components.

U.S. oil and natural gas companies operate a variety of telecommunications systems that are used to provide the internal communications capabilities that are crucial to protecting the safety of life, health, and property. These communications facilities are critical for the day-to-day operations of these companies, as well as for their response to potentially disastrous, life-threatening emergency situations. They are used for the direction of personnel and equipment, the control and synchronization of multiple geophysical acoustical signal sources for oil and gas exploration, and the telemetering of geophysical data. Mobile radio plays a critical role in providing communications for the management of individual wells; pipeline gathering systems; and in the transfer, loading, and delivery of petroleum products to end user consumers. In the event of emergency conditions, communication systems are essential to ensure the safety of personnel, the adjacent population, and the surrounding environment.

Petroleum and natural gas infrastructures are generally well equipped with gas-driven compressors and gas- or diesel-fired pumping facilities and backup generators that would enable the continued flow of natural gas, crude oil, and refined product deliveries for a limited time or that would implement a controlled shutdown following an interruption of electric power supply. There is also a possibility these backup generators may not function after an EMP event if they contain sensitive electronic components such as electronic control units. As one example of interdependency between the fuel and transportation sectors, we note that emergency generators that may keep critical electrical components of the petroleum and natural gas infrastructures running may become inoperative for lack of delivered fuel by a transportation sector short of fuels to run its trucks.

An electric power, water, or transportation disruption of short duration would not necessarily affect the operation of oil and natural gas infrastructure due to backup power and water resources. It is anticipated that crude oil and refined product deliveries could continue to flow for a few days, should these infrastructures be adversely affected. In the short term, natural gas deliveries are facilitated by the combined flexibility afforded by underground storage facilities and by line pack (the volume of gas maintained in the line at pressures above required delivery pressures). But outages of a few days or more can be expected to severely affect all infrastructure operations.

### **Recommendations**

The Federal Government should take the lead in identifying this threat to the oil and gas industry sectors and specify ways to mitigate its potential consequences.

- ◆ The Energy Information Sharing and Analysis Center (ISAC) should, with government funding, expand its mission to address EMP issues relative to the petroleum and natural gas industries. This would include facilitating a government/industry partnership in addressing policy, investment prioritization, and science and technology issues.
- ◆ The Federal Government should review the feasibility of establishing a national inventory of component parts for those items that would be either in great demand or have long lead times, to be made available in a catastrophic event such as an EMP incident.
- ◆ Protect critical components.
  - The oil and natural gas industries should develop resource lists of existing SCADA and process control systems, with prearranged contracts and potential suppliers in the event of an EMP incident.
  - A study should be performed that prioritizes critical facilities of the oil and gas sector for future hardening against EMP effects.
  - Industry should strongly urge its members that have not already done so to install backup control centers to provide operational continuity. Industry should also explore the site location decisions for backup control centers so that adequate geographic separation between the main site and the backup facility is provided to protect against simultaneous damage in the event of a single EMP event.
- ◆ Develop training and exercises.
  - Individual companies should consider engaging in regional response and recovery planning and exercises to deal with disruptions to physical and cyber infrastructures resulting from an EMP event.
  - Emergency response manuals should be revised to include periodically recurring EMP event training for current and future work force.
  - Detailed simulation of the petroleum and natural gas infrastructure on a regional or local basis should be performed to provide a more accurate assessment of the potential impact of EMP-induced damage to these infrastructures.
- ◆ Conduct research.
  - Research and development efforts should stress hardening of SCADA and other digital control systems equipment, both existing and new components, to mitigate the impact of a future EMP event. New standards for oil and gas control systems should be established with the industry to avoid potential damage from EMP effects. These efforts could best be accomplished by the participation of the various industry members, organizations (e.g., American Gas Association [AGA], Interstate Natural Gas Association of America [INGAA], Gas Technology Institute [GTI], American Petroleum Institute [API]), and government agencies.
  - A cost-benefit analysis should be conducted for protecting the commercial petroleum and gas infrastructure against the effects of an EMP. If the costs are estimated to be substantial, the Federal Government should defray a portion of these costs.

## Chapter 6. Transportation Infrastructure

### Introduction

Transportation has played an essential role in our development from scattered settlements to a modern nation. Maritime (i.e., oceanic) shipping sustained the first settlements some five centuries ago and remains the most important avenue for intercontinental commerce today. The 18th century saw the rise of canals in the eastern states, and interest in them lasted through the first decades of the 19th century. Later the railroad supplanted canals in the east and opened the western territories for large-scale economic development and settlement. The 20th century witnessed the advent of the airplane and the automobile, both of which have radically transformed our economy and society. Water, rail, road, and air transportation now bind us together as a nation—economically, socially, and politically.

The criticality of transportation, the impact of potential disruptions, and the need to address vulnerabilities has received national attention. As recognized by the President's National Security Telecommunications Advisory Committee (NSTAC) Information Infrastructure Group Report:<sup>1</sup>

- ◆ The transportation industry is increasingly reliant on information technology (IT) and public information-transporting networks.
- ◆ Although a nationwide disruption of the transportation infrastructure may be unlikely, even a local or regional disruption could have a significant impact. Because of the diversity and redundancy of the United States (U.S.) transportation system, the infrastructure is not at risk of nationwide disruption resulting from information system failure. Nonetheless, a disruption of the transportation information infrastructure on a regional or local scale has potential for widespread economic and national security effects.
- ◆ Marketplace pressures and increasing use of IT make large-scale, multimodal disruptions more likely in the future. As the infrastructure becomes more interconnected and interdependent, the transportation industry will increasingly rely on IT to perform its most basic business functions. As this occurs, it becomes more likely that information system failures could result in large-scale disruptions of multiple modes of the transportation infrastructure.
- ◆ There is a need for a broad-based infrastructure assurance awareness program to assist all modes of transportation.
- ◆ The transportation industry could leverage ongoing research and development initiatives to improve the security of the transportation information infrastructure.
- ◆ There is a need for closer coordination between the transportation industry and other critical infrastructures.

The transportation sector of the economy is often addressed as a single infrastructure, but in reality its various modes provide for several separate, but related, infrastructures. Rail includes the long-haul railroad and commuter rail infrastructures, air includes the commercial and general aviation infrastructures, road includes the automobile and trucking infrastructures, and water includes both the maritime shipping and inland waterway

---

<sup>1</sup> NSTAC Information Infrastructure Group Report, June 1999, <http://www.ncs.gov/nstac/reports/1999/NSTAC22-IIIG.pdf>.



infrastructures.<sup>2</sup> A combination of considerations—importance to the economy, potential for loss of life as a result of an electromagnetic pulse (EMP) attack, and criticality to civilian enterprises—has led us to focus on the long-haul railroad, trucking and automobile, maritime shipping, and commercial aviation infrastructures.

As far as transportation has developed, it is still far from static. The forces driving the continuing evolution of the transportation infrastructures can be understood in terms of the pursuit of competitive advantage, which derives from both lower cost and superior performance. Of particular importance, pressures for cost reduction have led to widespread adoption of just-in-time delivery practices. These practices not only reduce costs associated with maintaining large inventories, but also create strong dependencies on automated tracking of inventories and automatic sorting and loading to achieve efficient and reliable delivery of supplies and equipment. Just-in-time delivery is made possible by the application of technological advances in remote tracking, computer controls, data processing, inventory management, telecommunications, and uninterrupted movement. These technologies are all electronics-based and, hence, potentially vulnerable to EMP.

The imperative to achieve superior performance also has led to greater use of electronics, which has introduced a potential vulnerability to EMP. The automobile provides a familiar example of this phenomenon. Modern automobiles use electronics to increase engine performance, increase fuel efficiency, reduce emissions, increase diagnostic capability, and increase passenger safety and comfort.

To gauge the degree of vulnerability of the long-haul railway, trucking and automobile, maritime shipping, and commercial aviation infrastructures to EMP, the Commission has assessed selected components of these infrastructures that are vital to their operations. Our assessment is based on both data collected from testing conducted under the auspices of the Commission and other available test data that have direct applicability to transportation infrastructure assessment. For critical components of these infrastructures that we were unable to test—notably airplanes, air traffic control centers, locomotives, railroad control centers and signals, and ports—our assessment relies on surveys of equipment and communications links.

*The transportation infrastructures are trending toward increased use of electronics, thereby increasing potential EMP vulnerability.*

### Long-Haul Railroad

Railroads excel at carrying voluminous or heavy freight over long distances. Class I railroad freight<sup>3</sup> in 2003 totaled some 1.8 billion tons originated.<sup>4</sup> The major categories of

<sup>2</sup> Pipelines are sometimes associated with the transportation infrastructure but can be considered more usefully as part of the petroleum and natural gas infrastructures.

<sup>3</sup> The division of railroads into classes based on total operating revenue was a taxonomy defined by the Interstate Commerce Commission in the 1930s. The original threshold for a Class I railroad was \$1 million. In 2006, Class I railroads were those with operating revenues exceeding \$319.3 million. In North America, there are currently seven U.S. railroads that are defined as Class I, with an additional two Canadian railroads that would be considered Class I if U.S. definitions were applied. The old Class II and Class III designators are rarely used today. Instead, the Association of American Railroads speaks of regional railroads operating greater than 350 route-miles or generating more than \$40 million revenue, local line haul carriers with less than 350 route-miles and generating less than \$40 million revenue, and switching and terminal services carriers with highly localized functions, <http://www.railwest.com/railtoday.html>.

<sup>4</sup> “Tons originated” is a common term of art and index in the railroad industry used to track freight traffic volume. It is equal to the tons of traffic shipped by rail. Tons originated rail statistics are available from 1899.

freight carried by railroads, illustrated in **figure 6-1**, include coal, chemicals, farm products, minerals, food products, and a variety of the other goods essential to the operation of our economy.<sup>5</sup>

Coal dominates all other categories of freight, accounting for 44 percent of Class I railroad tonnage in 2003. More than 90 percent of this coal, some 700 million tons, is delivered annually to coal-fired power plants. Power plants that depend on railroad-delivered coal account for more than one-third of our electricity production. Today, these plants typically have only several days' to a month's supply of coal on site. While this reserve provides a useful buffer, under conditions of a prolonged failure of railroads to deliver coal, these plants would simply have to shut down.<sup>6</sup> Electricity production would be affected most in the Midwest, Southeast, and Southwest, regions more heavily dependent on coal-fired power plants.<sup>7</sup>

Railroads have achieved significant gains in efficiency and safety by modernizing and automating their operations. Today, freight railways are controlled and operated from a limited number of centralized control centers. For example, the western U.S. Union Pacific tracks are managed from Omaha, NE, and the Burlington Northern/Santa Fe tracks are managed from Dallas, TX. These centers, as well as operations throughout the rail system, use extensive communication networks for sensing, monitoring, and control. If a railroad control center becomes inoperable or loses communications with the rail network for any reason, all rail traffic in the affected domain will stop until communications are restored or backup procedures are implemented.

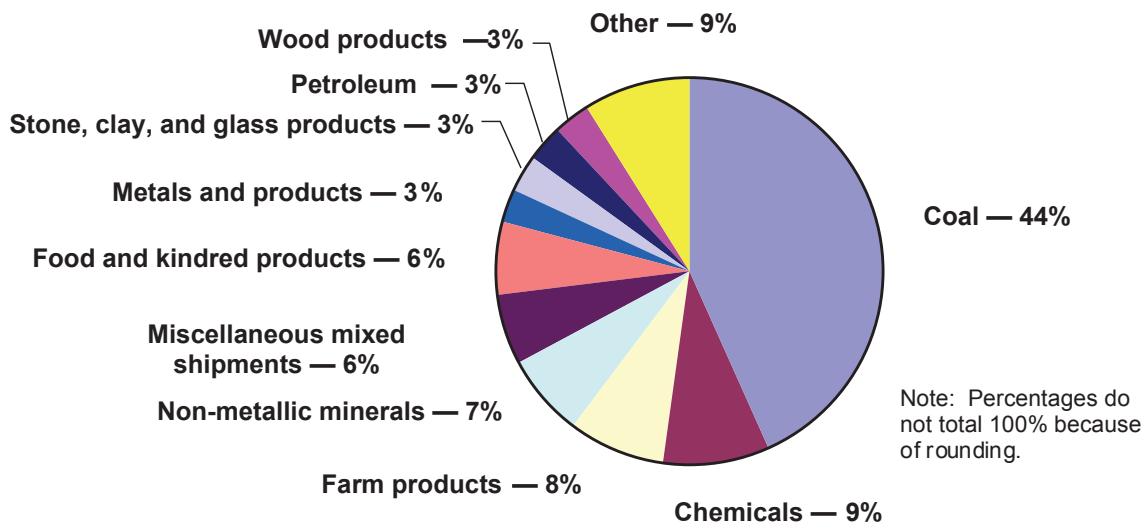


Figure 6-1. 2003 Class I Railroad Tons Originated

### ***EMP Vulnerability of the Long-Haul Railroad Infrastructure***

The principal elements of the railroad infrastructure that we assessed are railroad control centers, railroad signal controls, and locomotives.

<sup>5</sup> Association of American Railroads, <http://www.aar.org>.

<sup>6</sup> Some coal plants also can use natural gas, but this alternative fuel may not be available after an EMP attack. See Chapter 5, Petroleum and Natural Gas Infrastructures.

<sup>7</sup> Association of American Railroads, <http://www.aar.org>.

### *Railroad Control Centers*

We conducted an EMP vulnerability survey of CSX Transportation (CSXT), the railroad subsidiary of the CSX Corporation. CSXT operates the largest rail network in the eastern United States. Like the other major railroad companies, CSXT has centralized its critical control facilities in a single geographical area. The CSXT Jacksonville, FL, railroad control center includes three key nodes, each housed in a separate building—a customer service center, an advanced IT center, and a train dispatch center (**figure 6-2**). These buildings have no specific electromagnetic protection. About 1,200 trains are handled by the CSXT control center in a typical day.

Railroad control center operations rely on modern IT equipment—mainframe and personal computers, servers, routers, local area networks (LAN), tape storage units—some of which are similar to commercial off-the-shelf (COTS) equipment that has been EMP-tested. Based on this similarity, we expect anomalous responses of the IT equipment to begin at EMP field levels of approximately 4 to 8 kV/m. We expect damage to begin at fields of approximately 8 to 16 kV/m.



Figure 6-2. CSXT Train Dispatch Center

The CSXT railroad control center buildings rely on diesel power generators for standby power and central uninterruptible power supply (UPS) systems to provide continuous power to critical loads. Some buildings require chilled water for continuing computer operations. The buildings are interconnected by a fiber-optic ring and telephone lines. None of this equipment has specific EMP protection, and there are no data on the EMP vulnerability of this equipment.

The three railroad control center nodes are almost totally dependent on telephone lines (copper and fiber) for communications and data transfer. If all landlines fail, they still can communicate over a small number of satellite telephones, but data transfers would be severely limited.

Concerns about terrorist attacks and hurricanes have motivated CSXT to make provisions to operate for an extended period without support from the infrastructure. These provisions include diesel generators in case the two independent commercial power feeds should fail, fuel and food stored for 25 to 30 days of operation, beds for 50 people, and on-site wells to provide water.

*Based on our assessment and test results, a weak link in the railroad infrastructure is the railroad signal controls, which can malfunction and slow railroad operations following exposure to EMP fields as low as a few kV/m.*

In addition, all three of the key nodes have remote backup sites, either in Maryland or in the northern Midwest. This geographical dispersion provides some protection from a limited EMP attack. However, these backup sites rely on personnel in the Jacksonville

area for operations at the remote sites, which makes them dependent on the infrastructure for transporting their personnel. It is possible that their personnel could be transported over the CSXT rail system if air and road transportation was interrupted by an EMP attack. They also are dependent on commercial telephone service to transfer the Jacksonville telephone numbers to the alternate sites and to establish the alternate data links.

In the case of EMP-caused outages of the three key facilities and the failure of the backup sites, railroad operations would be severely degraded. Customers could not place shipping orders, data processing would cease, and, most important, train orders could not be generated. Train orders define the makeup of trains, their routes, and their priorities on the track. Trains cannot operate without orders and would revert to fail-safe procedures. The first priority would be to stop the trains. If it were apparent that the outages would last for more than a few hours, efforts would be made to move the trains to the yards. This process could take up to 24 hours.

Once the trains and their crews are secured, plans would be made to resume operations under manual procedures. Implementation of manual procedures could take several days or longer, during which time it would be difficult to operate at more than approximately 10 to 20 percent of normal capacity. Train orders can be issued manually using satellite telephones. The biggest challenge is maintaining communications with trains that are underway. Train yards can communicate with trains by radio. If the trains are within about 20 miles of the yard, the entire communication path is wireless. However, longer-range communications use landlines to repeater stations along the train routes. The repeater station batteries provide only about 24 hours of standby power.

Shipment of critical supplies likely could resume under manual control operations. Transporting food from farms to storage warehouses and from storage warehouses to cities would be a high priority. Trains also deliver chemicals that cities use to purify drinking water and treat waste water. As discussed above, power plants generally have some reserve of coal on hand, but eventually it would become crucial to resume coal shipments to power plants.

### *Railroad Signal Controls*

Railroads use two main types of controls: block controls and local controls. **Figure 6-3** shows a typical block signal control equipment enclosure and antenna. Block controls are used to assure that the next section (block) of track is clear before a train enters it. The main communications from the railroad control centers to the block controls uses a mix of radios and telephones. Block controls have battery backups that can sustain operations for up to 24 hours.

Local control systems manage grade crossings and signal both the train and the road traffic at a crossing. These control systems are designed to operate autonomously. Some modern local control systems have a minimal communications capability that consists of a telephone modem for fault reporting and possible downloading of programs and parameters for the controllers. Local control systems have battery back-up power, which would provide for normal operations from 8 to 48 hours, depending on the volume of train traffic.



**Figure 6-4** shows a typical local grade crossing control shelter and sensor connection. Local control systems have sensors bolted or welded directly to the rails. The resistance of the circuit, closed by the train wheels and axle, is measured and used to predict the train's arrival at the crossing. Modern systems are in shielded steel enclosures that include extensive surge protection.

Similar electronics technologies are used in both road and rail signal controllers. Based on this similarity and previous test experience with these types of electronics, we expect malfunction of both block and local railroad signal controllers, with latching upset beginning at EMP field strengths of approximately 1 kV/m and permanent damage occurring in the 10 to 15 kV/m range.

The major effect of railroad signal control failures will be delayed traffic. For centrally controlled areas of track, if block signals were inoperative, manual block authority would be implemented. Where possible, signal teams would be sent out to manually control failed switches. Crews also would set up portable diesel units to power railroad crossings that had lost power. Railroad crossing generators are on hand for emergencies, such as hurricanes. Repair and recovery times will be on the order of days to weeks. If commercial power is unavailable for periods longer than approximately 24 hours, degraded railroad operations will persist under manual control until batteries or commercial power is restored.



**Figure 6-3. Typical Block Signal Control Equipment Enclosure**



**Figure 6-4. Grade Crossing Shelter and Sensor Connection**

### *Locomotives*

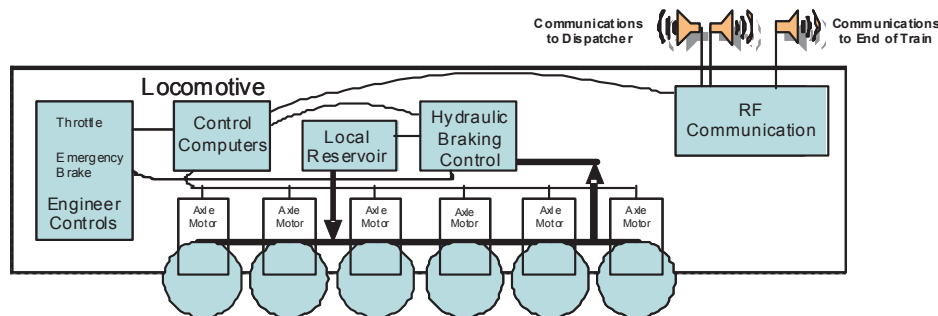
We conducted an assessment of diesel-electric locomotives at the GE Transportation Systems plant (one of two manufacturers of diesel-electric locomotives) in Erie, PA. Our assessment is based on a review of locomotive construction practices, operational procedures, and limited test data. While we do not have direct test data on EMP effects on diesel-electric locomotives, some data are available from a test of a locomotive of different



design that may provide some insight into the robustness of typical locomotive control electronics and subsystems.<sup>8</sup>

Two classes of locomotives were considered—those of the pre-microprocessor era and the more modern locomotives that make extensive use of electronic controls. Approximately 20 percent of the locomotive population is of the older generation; these are rapidly being replaced by the newer models. Electronics are not used to control critical functions in the older locomotives. We consider this generation of locomotives to be immune to EMP effects. While the locomotives themselves are considered immune, loss of communications with central dispatch or within the train requires that the engineer stop the train.

A block diagram showing the critical functions in the more modern locomotives is shown in **figure 6-5**. The major functions are traction (movement) and communications, both of which make extensive use of electronic components and, thus, are potentially vulnerable to EMP. As with older locomotives, the communications include communications to central dispatch and to other parts of the train. If these communications are lost for any reason, the train is required to stop.



**Figure 6-5. Modern Locomotive Functional Block Diagram**

The traction function is totally computer controlled, with the important exception of the engineer's emergency braking system. Three computers are used to control all major subsystems. Malfunction or loss of any of the computers will bring the train to a halt. Restoring operation could require the replacement of computers. Because few spare computers are provisioned, operations could be degraded until new computers are manufactured and installed—a process that could take months.

It is important to note that computer failure or total loss of power in the locomotives could cause loss of electrical control for the brakes. In this case, there is a totally independent, nonelectrical system that the engineer can activate to apply the brakes in both the engine and the cars, thereby halting the train. Therefore, even in the worst case, the engineer can stop the train and prevent train crashes.

Because we did not directly test EMP effects on diesel-electric locomotives, the EMP vulnerability levels can be estimated based only on existing data for computer network response, locomotive construction methods, and the limited data available from the previously referenced test on an electro-mechanical locomotive belonging to the Swiss Fed-

<sup>8</sup> Hansen, R.A., H. Schaer, D. Koenigstein, H. Hoitink, "A Methodology to Assess Exo-NEMP Impact on a Real System—Case Studies," EMC Symposium, Zurich, March 7 to 9, 1989. Reference describes EMP test of electro-mechanical locomotive belonging to Swiss Federal Railways.

eral Railroad.<sup>9</sup> Existing data for computer networks show that effects begin at field levels in the 4 to 8 kV/m range, and damage starts in the 8 to 16 kV/m range. For locomotive applications, the effects thresholds are expected to be somewhat higher because of the large metal locomotive mass and use of shielded cables. Therefore, we expect that effects will likely begin at incident field levels above the 20 to 40 kV/m range.

In summary, we consider the older generation of locomotives to be generally immune to EMP effects. Newer, electronically controlled locomotives are potentially more vulnerable. Based on construction practices, we expect that these vulnerabilities may manifest at EMP levels greater than 20 to 40 kV/m. While vulnerabilities may cause the locomotives to malfunction, fail-safe procedures ensure they can be stopped manually by engineers. Hence, we do not anticipate catastrophic loss of life following EMP exposure. Rather, we anticipate degraded operations, the severity of which depends on the incident EMP field levels. Normal locomotive operations can be restored on time scales from days to weeks or even longer. Restoration time scales could extend to months if computers, for which there are few spares, must be manufactured and replaced.

### **The Automobile and Trucking Infrastructures**

Over the past century, our society and economy have developed in tandem with the automobile and trucking industries. As a consequence, we have become highly dependent on these infrastructures for maintaining our way of life.

Our land-use patterns, in particular, have been enabled by the automobile and trucking infrastructures. Distances between suburban housing developments, shopping centers, schools, and employment centers enforce a high dependence on the automobile. Suburbanites need their cars to get food from the grocery store, go to work, shop, obtain medical care, and myriad other activities of daily life. Rural Americans are just as dependent on automobiles, if not more so. Their needs are similar to those of suburbanites, and travel distances are greater. To the extent that city dwellers rely on available mass transit, they are less dependent on personal automobiles. But mass transit has been largely supplanted by automobiles, except in a few of our largest cities.

As much as automobiles are important to maintaining our way of life, our very lives are dependent on the trucking industry. The heavy concentration of our population in urban and suburban areas has been enabled by the ability to continuously supply food from farms and processing centers far removed. Today, cities typically have a food supply of only several days available on grocery shelves for their customers. Replenishment of that food supply depends on a continuous flow of trucks from food processing centers to food distribution centers to warehouses and to grocery stores and restaurants. If urban food supply flow is substantially interrupted for an extended period of time, hunger and mass evacuation, even starvation and anarchy, could result.

Trucks also deliver other essentials. Fuel delivered to metropolitan areas through pipelines is not accessible to the public until it is distributed by tanker trucks to gas stations. Garbage removal, utility repair operations, fire equipment, and numerous other services

---

<sup>9</sup> The Swiss executed both free-field (up to 25 kV/m) and current-injection (up to 2 kA) tests on a 4.6 MW, 80-ton electro-mechanical locomotive in both power-on and power-off configurations. During the free-field illumination, the test report states that "important analog/digital control electronics, deep inside the PC-boards, was repeatedly burnt out."

are delivered using specially outfitted trucks. Nearly 80 percent of all manufactured goods at some point in the chain from manufacturer to consumer are transported by truck.

The consequences of an EMP attack on the automobile and trucking infrastructures would differ for the first day or so and in the longer term. An EMP attack will certainly immediately disable a portion of the 130 million cars and 90 million trucks in operation in the United States. Vehicles disabled while operating on the road can be expected to cause accidents. With modern traffic patterns, even a very small number of disabled vehicles or accidents can cause debilitating traffic jams. Moreover, failure of electronically based traffic control signals will exacerbate traffic congestion in metropolitan areas. In the aftermath of an EMP attack that occurs during working hours, with a large number of people taking to the road at the same time to try to get home, we can expect extreme traffic congestion. Eventually, however, people will get home and roads will be cleared as disabled cars are towed or pushed to the side of the road.

Our test results show that traffic light controllers will begin to malfunction following exposure to EMP fields as low as a few kV/m, thereby causing traffic congestion. Approximately 10 percent of the vehicles on the road will stop, at least temporarily, thereby possibly triggering accidents, as well as congestion, at field levels above 25 kV/m.

After the initial traffic congestion has subsided, the reconstitution of the automobile and trucking infrastructures will depend primarily on two factors—the availability of fuel and commercial power. Vehicles need fuel and service stations need electricity to power pumps. Few service stations have backup generators. Thus, replenishing the fuel supply and restoring commercial power will pace the return to normal operations. Similarly, restoration of traffic control systems will depend on the availability of commercial power and on the repair of damaged traffic control signals.

### **EMP Vulnerability of the Automobile and Trucking Infrastructures**

We tested the EMP susceptibility of traffic light controllers, automobiles, and trucks.

#### *Traffic Light Controllers*

The road traffic control system is composed of sensors, control, and output systems. **Figure 6-6** shows a typical signalized intersection.



**Figure 6-6. A Typical Signalized Intersection**

Control systems are implemented according to one of several specifications that have evolved over the years. We performed tests of 170E type controllers, in use in approximately 80 percent of signalized intersections. We tested a single controller box populated by multiple electronics cards. In the course of the testing, various cards were damaged and subsequently replaced to continue the testing. Four different types of effects were observed during intersection controller tests:

1. Forced Cycle: At field levels of 1 to 5 kV/m, the light was forced to cycle from green to red without going through yellow. This is a transient effect that recovers automatically after one cycle.
2. Disrupted Cycle: At field levels of 5 to 10 kV/m, the normally programmed cycle times became corrupted and change to a cycle different from that originally programmed. The controller had either been damaged or needed to be manually reset.
3. No Cycle: At 10 to 15 kV/m, the side street lights at an intersection never turned green. The controller had been damaged.
4. Flash Mode: Also at 10 to 15 kV/m, the intersection went into a mode in which the lights in all directions were flashing. This mode can cause large traffic jams because traffic flow is severely reduced in this situation. The controller has either been damaged or needs to be manually reset.

Based on these results, we anticipate that EMP will trigger moderate to severe traffic congestion in metropolitan areas. The traffic congestion may be exacerbated by the panic reactions possibly attendant to an EMP attack. None of the data predict or suggest life-threatening conditions; conflicting green lights did not occur during our tests. All the observed effects would cause less traffic disruption than would a power outage, which results in no working traffic lights.

The highway network's dependency on electrical power was demonstrated during Hurricane Isabel in 2003. Although some critical intersections were equipped with back-up power supplies, they typically were operational only for 24 hours. In many localities, during power outages, law enforcement officers were required to control the critical intersections. As such, these officers were taken away from other activities that they could be serving during emergencies.

Reestablishing normal traffic flow depends on the severity of the EMP-induced faults. Manual resets for all traffic signals in a medium-sized city (population of 500,000) can be accomplished in approximately a day, assuming available personnel.<sup>10</sup> The timeline for repairing damaged traffic controller boxes depends on the availability of spare parts. The timeline for either manual resets or repairs under stressed conditions are unknown.

Major metropolitan areas are establishing traffic operations centers (TOC) as an integral part of their traffic control infrastructure. A city's TOC is responsible for downloading the parameters controlling traffic signal timing and traffic signal coordination. However, a TOC is not a critical node from a traffic control standpoint. If the center were to become inoperable, the immediate effect would be on the city's integrated traffic system; the city would not be able to monitor its roadways, use its variable message signs along priority roadways such as interstates, or produce content for the cable channels or Internet updates that provide the public with information on traffic and highway conditions. The primary long-term effect of a TOC failure would be a gradual drifting of the signal timing synchronization that the center provides to the intersections to which it connects.

---

<sup>10</sup> Conversation with Colorado Springs lead traffic engineer.

### *Automobiles*

The potential EMP vulnerability of automobiles derives from the use of built-in electronics that support multiple automotive functions. Electronic components were first introduced into automobiles in the late 1960s. As time passed and electronics technologies evolved, electronic applications in automobiles proliferated. Modern automobiles have as many as 100 microprocessors that control virtually all functions. While electronic applications have proliferated within automobiles, so too have application standards and electromagnetic interference and electromagnetic compatibility (EMI/EMC) practices. Thus, while it might be expected that increased EMP vulnerability would accompany the proliferated electronics applications, this trend, at least in part, is mitigated by the increased application of EMI/EMC practices.

We tested a sample of 37 cars in an EMP simulation laboratory, with automobile vintages ranging from 1986 through 2002. Automobiles of these vintages include extensive electronics and represent a significant fraction of automobiles on the road today. The testing was conducted by exposing running and nonrunning automobiles to sequentially increasing EMP field intensities. If anomalous response (either temporary or permanent) was observed, the testing of that particular automobile was stopped. If no anomalous response was observed, the testing was continued up to the field intensity limits of the simulation capability (approximately 50 kV/m).

Automobiles were subjected to EMP environments under both engine turned off and engine turned on conditions. No effects were subsequently observed in those automobiles that were not turned on during EMP exposure. The most serious effect observed on running automobiles was that the motors in three cars stopped at field strengths of approximately 30 kV/m or above. In an actual EMP exposure, these vehicles would glide to a stop and require the driver to restart them. Electronics in the dashboard of one automobile were damaged and required repair. Other effects were relatively minor. Twenty-five automobiles exhibited malfunctions that could be considered only a nuisance (e.g., blinking dashboard lights) and did not require driver intervention to correct. Eight of the 37 cars tested did not exhibit any anomalous response.

Based on these test results, we expect few automobile effects at EMP field levels below 25 kV/m. Approximately 10 percent or more of the automobiles exposed to higher field levels may experience serious EMP effects, including engine stall, that require driver intervention to correct. We further expect that at least two out of three automobiles on the road will manifest some nuisance response at these higher field levels. The serious malfunctions could trigger car crashes on U.S. highways; the nuisance malfunctions could exacerbate this condition. The ultimate result of automobile EMP exposure could be triggered crashes that damage many more vehicles than are damaged by the EMP, the consequent loss of life, and multiple injuries.

### *Trucks*

As is the case for automobiles, the potential EMP vulnerability of trucks derives from the trend toward increasing use of electronics. We assessed the EMP vulnerability of trucks using an approach identical to that used for automobiles. Eighteen running and nonrunning trucks were exposed to simulated EMP in a laboratory. The intensity of the EMP fields was increased until either anomalous response was observed or simulator limits were reached. The trucks ranged from gasoline-powered pickup trucks to large diesel-powered tractors. Truck vintages ranged from 1991 to 2003.



Of the trucks that were not running during EMP exposure, none were subsequently affected during our test. Thirteen of the 18 trucks exhibited a response while running. Most seriously, three of the truck motors stopped. Two could be restarted immediately, but one required towing to a garage for repair. The other 10 trucks that responded exhibited relatively minor temporary responses that did not require driver intervention to correct. Five of the 18 trucks tested did not exhibit any anomalous response up to field strengths of approximately 50 kV/m.

Based on these test results, we expect few truck effects at EMP field levels below approximately 12 kV/m. At higher field levels, 70 percent or more of the trucks on the road will manifest some anomalous response following EMP exposure. Approximately 15 percent or more of the trucks will experience engine stall, sometimes with permanent damage that the driver cannot correct.

Similar to the case for automobiles, the EMP impact on trucks could trigger vehicle crashes on U.S. highways. As a result, many more vehicles could be damaged than those damaged directly by EMP exposure.

### **Maritime Shipping**

The key elements of the maritime infrastructure are ocean-going ships and their ports. We did not perform an EMP assessment of ships.

There are more than 100 major public ports in the United States located along the Atlantic, Pacific, Gulf of Mexico, and Great Lakes coasts, as well as in Alaska, Hawaii, Puerto Rico, Guam, and the U.S. Virgin Islands. Deep-draft ports accommodate ocean-going vessels, which move more than 95 percent of U.S. overseas trade by weight and 75 percent by value.<sup>11</sup>

Ports handle a variety of cargo categorized as bulk cargo, including liquid bulk (e.g., petroleum) and dry bulk cargo (e.g., grain); break bulk cargo in barrels, pallets, and other packages; and general cargo in steel containers. Major commodities shipped through U.S. ports include:<sup>12</sup>

- ◆ Crude petroleum and petroleum products—oil and gasoline
- ◆ Chemicals and related products—fertilizer
- ◆ Coal—bituminous, metallurgical, and steam
- ◆ Food and farm products—wheat and wheat flour, corn, soybeans, rice, cotton, and coffee
- ◆ Forest products—lumber and wood chips
- ◆ Iron and steel
- ◆ Soil, sand, gravel, rock, and stone

### **Port Operations**

Our assessment of maritime shipping infrastructure focuses on ports. EMP assessments were conducted for the Port of Baltimore in Maryland and ports in the Hampton Roads, VA, area. The Port of Baltimore assessment was performed at the Seagirt and Dundalk Marine Terminals. The assessment was hosted by the Maryland Port Administration. The Hampton Roads assessment was hosted by the U.S. Coast Guard (USCG) and conducted

---

<sup>11</sup> American Association of Port Authorities, <http://www.aapa-ports.org>.

<sup>12</sup> Ibid.

at their offices in Portsmouth, VA, and at the Norfolk International Terminal (NIT) in Norfolk—one of three terminals in the Hampton Roads area.

Under Coast Guard mandate, the National Vessel Movement Center (NVMC) was established to track notice of arrival information from ships entering all U.S. ports. The NVMC is located in Kearneyville, WV. All cargo ships greater than 300 gross tons must notify the NVMC at least 96 hours prior to their arrival.

For the ports of Baltimore and Hampton Roads, communications between ships and between ship and shore are primarily by way of very high frequency (VHF) radio. All vessels are required to monitor Channel 16 (156.8 MHz). A system of repeaters allows VHF communications 25 miles off shore. Some vessels have satellite communication systems. All vessels are brought into the ports by a pilot who boards the ship in open water.

#### *Hampton Roads Area Port*

NIT, one of the Hampton Roads area facilities, operates much like a bus stop. Ships with 2,000 to 4,000 containers arrive any hour of the day, any day of the week. A few hundred containers may be offloaded and additional containers loaded onboard. Then, after only 4 to 8 hours in port, the ship sails on to its next port. Most of the ships have regular routes. Some ships (15 percent) contain break bulk cargo, which is packaged cargo not in containers. The third type of cargo is bulk (like coal); however, NIT does not handle bulk cargo.

Containers are loaded on and off the vessels using sophisticated cranes designed specifically for the purpose (**figure 6-7**). The containers typically are loaded onto the chassis of yard trucks that shuttle them to storage locations around the port. In some cases “straddle carriers” are used instead of yard trucks.



**Figure 6-7. Container Cranes and Stored Containers**

Cranes are the key element in the operation of the terminal. The criticality of the cranes is underscored by the fact that repair crews are kept on site at NIT at all times. Repairs are required to be made in 15 minutes or less. Cranes have more than 100 computers and sensors in them. Replacement parts for normally anticipated failures are warehoused on site. However, the numbers of spares are not planned in anticipation of an EMP attack.

Each container has a unique identification number. The container number is noted when it is unloaded from a ship. When it is placed in the yard by one of the yard trucks (or straddle carriers), its parking place is sent to the data center in Portsmouth through a handheld wireless computer. All the container location data are mirrored to the data center at NIT and backed up daily. The data centers have UPS and diesel backup power. Per-

sonnel also walk the yard to reconfirm the accuracy and completeness of the container locations. There are typically 30,000 to 40,000 containers stored at NIT.

Eventually, the container is loaded onto a road truck or rail car for shipment to its destination. A container number is logged whenever the container passes through the entrance area. The final checkpoint has radiation detectors to look for radioactive materials that might be moved out of the terminal.

### *Port of Baltimore*

The 275-acre Seagirt Marine Terminal is exclusively a container terminal. On the land side, containers arrive and leave primarily by truck (95 percent), even though the terminal is adjacent to CSX railroad's Intermodal Container Transfer Facility (ICTF). Seagirt has seven active electric cranes for loading and unloading ship containers. Like NIT, the Seagirt cranes rely on commercial power for their operation.

Nearby Dundalk Marine Terminal is more than twice as large (570 acres) and has a mixture of cargo types: passengers on cruise ships, containers, roll-on/roll-off (ro-ro), and break bulk. Dundalk does not process bulk cargo. The terminal has 10 dockside container cranes, which are of various vintages, all older than the Seagirt cranes. The Dundalk dockside cranes all use diesel-powered electric motors.

Dundalk docks on the channel next to Seagirt are used for ro-ro and break bulk cargos. Ro-ro cargos include automobiles and a large assortment of farm and construction equipment.

Both marine terminals use an assortment of diesel- and diesel/electric-powered equipment to move containers around the yard and onto and off of trucks and railroad cars. Diesel-powered top loaders are used to move and stack containers. **Figure 6-8** shows two of the six diesel/electric-powered rubber tire gantries (RTG) at Seagirt. They provide a more efficient method than the top loaders for moving and stacking containers. Unlike the dockside cranes, whose motion is limited by fixed rails, RTGs can be moved and placed strategically around the terminal.



Figure 6-8. RTG at Seagirt Marine Terminal

Information about the containers is transmitted to a central computer unit in the Seagirt computer room using wireless handheld Teklogix units (**figure 6-9**). Information about the status and storage location of each container is stored in the database using input from the handheld units. Conversely, the handheld unit operators can download information about any container from the central database. The container tracking systems at Seagirt and Dundalk are highly automated. Their operation is essentially paperless, which places heavy reliance on the integrity of the databases. To enhance reliability, all critical data are mirrored in near-real time to a nearby backup site (about 1 mile away). In addition, backup tapes are generated every evening. Seven days of backups are maintained at the backup site. The computer room uses a Liebert UPS for short-term backup power. Long-term emergency power is provided by a diesel generator. Because the current unit proved



Figure 6-9.  
Handheld  
Wireless Data  
Unit

to be inadequate during a lightning-induced power outage, a new diesel generator is being installed. The new unit also will provide emergency power to critical equipment outside the computer room.

The land side of operations at Seagirt and Dundalk Marine Terminals is primarily concerned with controlling the ingress and egress of container trucks. Entry is regulated by a series of manned consoles overlooking the truck entry area (**figure 6-10**). Trucks pull up to speaker boxes where the driver provides information about the company, vehicle, and business at the terminal. Operators use remote cameras to read license plate numbers and other vehicle identification markings.

The operator enters the information into the database and is issued a routing slip that is printed near the speaker box. The slip looks similar to an airline boarding pass and contains information about the truck and the container with which it is concerned. The driver then proceeds to a manned checkpoint directly below the entry control consoles. Here, Seagirt personnel examine the routing slip and check the driver's identification before allowing the truck to proceed into the terminal to pick up or drop off a container. A similar check is performed when the truck leaves the terminal. All operations are entered into a database, providing real-time information on the status of each truck and its container. There are typically 1,600 truck operations a day at Seagirt.



Figure 6-10. Truck Control Station

### ***EMP Vulnerability of Maritime Shipping***

An EMP event could affect operations in every phase of the transfer of container cargo from ships at sea to the highways and rails of the United States. The ability to provide information on the cargo and crew 96 hours before reaching all ports in the United States could be degraded by EMP-induced failures at the NVMC. Even if the NVMC is not directly impacted by EMP, the ability of ships and their agents to communicate with the NVMC could be affected by a failure in the telephone system.

The USCG, under the authority of the captain of the port, can allow ships into port without a formal notification to the NVMC. The USCG would likely send one of its cut-



ters to contact ships at sea by VHF radio. Its crew might board the ship and escort it to port. The choice of which ships to allow in and which to stop would be at the discretion of the USCG. Depending on the extent of the EMP-affected areas, ships might also be diverted to alternate ports.

Ships approved to enter port still need a pilot to navigate the inner waterways. Pilots use their own boats to reach the ships and use VHF radios for communication. It is unlikely that all the pilot boats and their radios would be damaged by an EMP event. There are always some that are not operating at any given time. Pilots normally rely on satellites for navigation, but they are capable of navigating using charts and buoys.<sup>13</sup>

An EMP event could slow down the arrival of ships to port, but it would not necessarily stop all arrivals. This was the case for the terminals in the Hampton Roads area after September 11, 2001. The terminals remained open, but the USCG was aggressive in boarding and escorting ships to port.

Once container ships are in port, they are dependent on the dockside cranes to load and unload containers. Most of the container cranes in the Hampton Roads area are powered by commercial power; the few remaining diesel-powered cranes are being replaced by electric cranes. All

*Dockside cranes are electrically powered from commercial power with no backup power source; loss of commercial power caused by EMP exposure would halt loading and unloading until electric power service is restored.*

the dockside cranes at Seagirt also are powered by commercial power. The cranes using commercial power have no backup for commercial power. Thus, loading and unloading of containers would stop at these docks until commercial power is restored. The 10 dockside cranes at Dundalk Marine Terminal are diesel/electric and independent of commercial power.

EMP might damage the container cranes. The cranes have myriad electrical components—programmable logic controllers, sensors, and motors. However, given their height, it is likely that they are struck frequently by lightning. While repair crews and replacement parts are kept on site at all times, these parts are unlikely to be sufficient to meet the replacement needs after an EMP attack.

Once containers are removed from a ship, they are placed in the yard in a numbered parking spot or in block storage, where canisters are stacked together like on a ship. Diesel powered yard trucks and straddle carriers are used for this purpose. It is unlikely that all of them would be damaged beyond repair by an EMP event. There are always units that are not operating, which, based on the test data taken on automobiles and trucks, would make them less likely to be damaged.

Equipment not damaged by EMP will be able to operate as long as it has diesel fuel. Typically, a 10-to-20 day supply of fuel is stored at the terminals. They normally rely on commercially powered electric pumps to move fuel out of the storage tanks, but would improvise alternate methods if there was an extended outage of commercial power.

The actual delivery and removal of containers from the ports is dependent on outside trucks and, to a lesser extent, railroads. Diesel/electric RTGs are used to move containers

<sup>13</sup> Many satellites are likely to be unaffected by either EMP or by enhanced space radiation environment produced by a high-altitude burst (see Chapter 10 of this volume), but there may be some degradation as a result of vulnerabilities of receivers or ground stations.



on and off trucks and rail cars. While RTGs are the most efficient method for moving containers, in the event they all failed, it is possible to load and unload containers with diesel-powered top loaders. Even ordinary forklifts could be used in an emergency. Ro-ro operations are less dependent on the operation of terminal equipment. Cranes are not used to unload the equipment—it just rolls down a ramp. Some break bulk cargo ships have their own cranes for dockside operations.

Container-handling equipment is only part of the port operations process. Record keeping is as important. Each container arriving at the port must be tracked until it leaves the port. If the records are lost, reconciling claims of lost containers could have a significant economic impact.

The location of each canister at the Hampton Roads area ports is stored in a database at a data center in Portsmouth. The data are mirrored to the data center at NIT and backed up daily. Both data centers have a UPS and backup generators. They rely on telephone lines to receive data and to communicate with each other.

It is unlikely that both data centers would be so damaged by EMP that they could not operate. They use multiple personal computers from different manufacturers to process the data. The NIT data center, which was visited as part of the assessment, uses Windows<sup>®</sup> software for some applications and Macintosh<sup>®</sup> software for others. This diversity in location, hardware, and software makes it less likely that there will be a total failure of the data processing system.

Even if all data on the container locations were to be lost, it would be possible to regenerate it in a few days. Personnel routinely roam the yard checking the accuracy of the database. They compare the container's unique number with the number of the parking spot. These personnel could reverse the process and regenerate the database.

The arrangement is similar at the Seagirt and Dundalk Marine Terminals. They have a central computer room with multiple servers that support the critical databases. The computer room also contains the base station for the wireless handheld units, various routers, and myriad telephone cables. There is no shielding that would limit EMP coupling to the large number of cables in the room. EMP-induced upsets should be expected and damage is certainly possible.

Critical data are mirrored to another data center about 1 mile away and backed up daily. Both data centers have a UPS and backup generators. The backup generator at Seagirt is inadequate to maintain operations and is being replaced with a more powerful unit that also will provide backup power to other critical equipment, such as the speakers and cameras at the truck gates.

It is unlikely that both of the Baltimore area data centers would be so damaged by EMP that they could not operate. They use multiple personal computers of different generations and from different manufacturers to process the data. The diversity in location and hardware makes it less likely that there will be a total failure of the data processing system. Paper records also would be needed to track the containers entering and leaving both the land and sea sides of the port. The ports could operate at significantly reduced capacity using a paper-based tracking system if necessary. It likely would take several days to implement the process.

Successful recovery from an EMP event will depend greatly on the availability of power and the ability of the USCG and port personnel to evaluate their situation and

---

modify their operations accordingly. The events of September 11, 2001, and the need to survive periodic hurricanes have fostered the type of planning needed to respond to an EMP event. Although EMP was not directly considered, many of the plans for emergency recovery would be helpful after an EMP event.

During the assessment, it was encouraging that people in authority were clearly capable of responding well to unexpected situations. However, their response to an EMP event could improve significantly if they had a better understanding of what to expect.

### Commercial Aviation

Air travel has become ingrained in our way of life. There were 72 U.S.-certified airline carriers at the end of 2002, employing 642,000 pilots, flight attendants, mechanics, and other workers. U.S. airlines carried 560 million domestic passengers during 2001, logging some 700 billion passenger miles. In addition, U.S. airlines all carry freight to some extent. Commercial air freight shipments totaled about 22 billion ton-miles.<sup>14</sup>

The key elements of commercial aviation infrastructure that we assessed are the air traffic control system and the aircraft themselves.

The Federal Aviation Administration (FAA) has the responsibility for operating the U.S. air traffic control system with an emphasis on passenger safety. The FAA rigorously controls commercial air traffic—on the ground at airports (by airport towers), all takeoffs and landings (by Terminal Radar Approach CONTROL—TRACONS), and all en route travel (by air route traffic control centers—ARTCCs). Two essential parts of the FAA air traffic control architecture are (1) command and control through communication among controllers and between controllers and pilots, and (2) navigation aids for following proper routes, terminal approaches, and landing.

Commercial air traffic in U.S. airspace at altitudes up to 70,000 feet is controlled at all times. U.S. airspace is divided into 24 regions, 21 for the contiguous states and one each for Alaska, Hawaii, and Guam. Each region is controlled by an ARTCC. These centers provide en route control for aircraft at altitudes above 17,000 feet, maintaining safe separation between aircraft and routing aircraft around bad weather. Terminal control is provided for aircraft at lower altitudes and on the ground by airport towers.

An ARTCC has an operations room (**figure 6-11**) that consists of rows (banks) of individual controllers. The region controlled by a center is divided into sections. Aircraft are tracked and controlled by individual controllers and handed from controller to controller as the aircraft moves from section to section. Control passes from ARTCC to ARTCC over a dedicated private network telecommunications link that connects a controller from one facility to the next controller at another



Figure 6-11. An ARTCC Operations Room

<sup>14</sup> Bureau of Transportation Statistics.

facility. En route control is acquired and handed off to a terminal controller in a similar manner.

If terminal control is interrupted, en route control takes over. If an en route control center is interrupted, control is turned over to another en route control center. These protocols provide redundant backup capability.

Radars are used to acquire and track aircraft in support of air traffic control centers. Generally, multiple radars will track an aircraft. Computers in air traffic control centers process radar information to form mosaic sectional displays and pass aircraft tracking information from center to center and across sections at a control center. Visualization is with a cathode ray tube (CRT) screen; paper printouts are also provided and used as a backup. Given a large number of radars with overlapping coverage, failure of a single radar will not adversely affect commercial air operations. Simultaneous failure of multiple radars, as could happen in an EMP attack, could shutdown all air traffic in the affected region, possibly nationwide.

The commercial aircraft in use are primarily jet-powered aircraft constructed by Boeing in the United States, and Airbus in Europe. In addition, there are various manufacturers of smaller commuter aircraft.

More than any other transportation infrastructure, the commercial aviation infrastructure is based on electronics. Everything from fly-by-wire aircraft flight control systems to navigation, communications, engine sensors and controls, and essential ground-based operations depends on microprocessor computer control.

Although a shutdown or curtailment of commercial aviation would have a severe, perhaps crippling, impact on the airline industry itself, the consequences for critical infrastructures would be less serious. Few vital economic activities are highly dependent on the unique advantage—speed—that commercial air transport has over the various modes of land transport.

### ***EMP Vulnerability of the Commercial Aviation Infrastructure***

#### ***Aircraft***

Our commercial aircraft EMP assessment was conducted based on results of a meeting and subsequent discussions with Boeing electromagnetics effects (EME) staff. This staff is responsible for assuring that Boeing commercial aircraft can operate following exposure to nonhostile electromagnetic (EM) environments. Specifically, we assessed the amount of EMP protection that might be afforded by protection against lightning and high-intensity radiated fields (HIRF). Moreover, our assessment focused on safety of flight and the capability to land a plane after EMP exposure. We did not address continuation of normal flight operations, because we expect that all aircraft will be directed to land immediately on notification of an EMP attack.

Boeing maintains a strict engineering protocol for assuring their commercial aircraft are protected against nonhostile EM environments. This protocol includes qualification testing that is a function of flight-critical electronics categories, application of immunity standards to electronics boxes (sometimes referred to as line-replaceable units [LRU]), and hardening practices tailored to specific requirements.

*EME Qualification Practices for Safety-of-Flight Electronics.* Boeing assigns electronics equipment to categories to differentiate the impact of loss of function. The highest category is reserved for electronics boxes, the failure of which would be considered catastrophic, and could lead to potential loss of the aircraft. Because our assessment focused on safety of flight, this is the most important category for EMP effects.

For this category of electronic subsystems, EME qualification is performed by a combination of low-level system tests and electronics box immunity tests (see next section). The purpose of the system-level tests is to estimate the intensity of the electromagnetic stresses coupled to the electronics box interfaces (connectors). For lightning (the EM environment most similar to EMP), the box immunity tests are then used to demonstrate that the electronics immunity levels are at least a factor of two higher than the coupled stresses. If this margin is not achieved, Boeing adjusts the protection tactics until this requirement is met. For lower-criticality electronic systems, only the box immunity tests are conducted, and there is no explicit relationship to the coupled stress required.

◆  
*Although commercial aircraft have proven EM protection against naturally occurring EM environments, we cannot confirm safety of flight following EMP exposure. Moreover, if the complex air traffic control system is damaged by EMP, restoration of full services could take months or longer.*

There has been significant evolution in the use of electronics in commercial aircraft. For aircraft designs prior to the 777, a direct mechanical/hydraulic link to the control surfaces was maintained, thereby minimizing electronics criticality for safety-of-flight applications. This observation would mitigate in favor of inherent EMP immunity for the nonelectronic subsystems. However, depending on aircraft, there are still some flight-critical functions performed by electronics, for which EMP immunity is not known. Therefore, even for pre-777 designs, there are insufficient data to confirm EMP immunity. Additional testing (limited to flight-critical electronics) is required to confirm EMP immunity. This testing should include low-level system testing to estimate EMP stresses at electronics interfaces and the corresponding electronics immunity testing. The recommended approach is essentially an extension of the existing lightning protocol to provide coverage for the EMP environment.

Boeing considers the 777 to be their first fly-by-wire design, incorporating more flight-critical electronics than used in earlier designs. Therefore, the newer designs may be more prone to EMP safety-of-flight impact. This potential is significantly mitigated by judicious use of redundancy for flight-critical subsystems. For example, while the flight-control systems use electrical signals rather than mechanical wires for control surface instructions, the primary digital controls are backed up by analog signals. Moreover, significant redundancy (up to four levels) is built into each flight-control subsystem. Therefore, the possible EMP susceptibility is offset significantly by careful, redundant design. Nonetheless, the qualification protocols do not provide adequate coverage for anticipated EMP responses. Therefore, as is the case for the earlier designs, additional testing is required to confirm EMP immunity. This testing should address both the EMP stresses at electronics interfaces and the corresponding immunity testing. Because there is more application of electronics in the newer designs, more extensive testing will be required than for the earlier designs.



*EME Immunity Testing Standards.* The industry standard for electronics immunity testing for commercial aircraft is RTCA/DO-160D.<sup>15</sup> Boeing uses an internal standard that flows down from RTCA/DO-160D but is tailored to the company's technical practices. For lightning, damped sinusoid immunity testing at center frequencies of 1 and 10 MHz is required. Other EMP aircraft testing has shown that EMP response tends to be at higher frequencies, generally in the 10 to 100 MHz range. In addition, conducted susceptibility HIRF testing is required for frequencies covering and extending far beyond the EMP range. However, the test amplitudes are lower than might be expected for EMP. Therefore, EMP survivability cannot be directly inferred from commercial aircraft lightning and HIRF immunity testing standards.

*EME Hardening Practices.* EME hardening in Boeing aircraft is achieved using a combination of tactics-stress reduction (e.g., use of shielded electrical cables), redundancy of flight-critical systems (depending on the system, up to four channels of redundancy are applied), and software error detection/correction algorithms for digital data processing. The combination of these tactics is adjusted to match the specific requirements of different electronic subsystems. In addition, hardening measures may be applied to electronic boxes to increase immunity, if required, to meet the Boeing specifications that flow down from DO-160D.

In summary, the Boeing engineering approach for protection and qualification against nonhostile electromagnetic environments is well established, and it is demonstrated by experience to be sufficient for the EM environments to which the aircraft are exposed during normal operations. While these procedures may provide significant protection in the event of an EMP attack, this position cannot be confirmed based on the existing qualification test protocols and immunity standards. This conclusion is applicable to all commercial aircraft currently in service, including the earlier designs. However, it is particularly emphasized for the newer, fly-by-wire designs that, by virtue of more reliance on digital electronics, may be more prone to EMP effects.

#### *Air Traffic Control*

We conducted an EMP vulnerability assessment of air traffic control by discussions with FAA engineers and former air traffic controllers and by visits to an FAA facility in Oklahoma City and the ARTCC in Longmont, CO. Moreover, because computer networks are integral parts of the air traffic control system, existing EMP test data on similar COTS electronics is applicable. Our testing did not include the FAA's private telecommunications network links connecting the ARTCCs, such as the FAA Leased Interfacility National Air Space Communications System (LINCS) and more recently the FAA Telecommunications Infrastructure (FTI) Program.<sup>16</sup> These FAA critical telecommunications

<sup>15</sup> RTCA, Inc., is a not-for-profit corporation that develops recommendations regarding communications, navigation, surveillance, and air traffic management system issues.

<sup>16</sup> The FAA LINCS is a highly diverse private network constructed to meet specific requirements of a customer with critical mission requirements. The FAA LINCS is the most available private line network in the world with an off-backbone availability requirement of 99.8 percent. More than 21,000 circuits serve the entire network. More than 200 circuits form the LINCS backbone and satisfy diversity requirements of 99.999 percent availability. Despite natural disasters, major failures of public infrastructures, and the 2001 terrorist attacks, the FAA LINCS survived as designed, keeping the line of communication open between air traffic controllers and airplanes. In July 2002, the FAA initiated a substantial modernization of its telecommunications networks to meet its growing operational and mission support requirements and to provide enhanced security features. The new FTI Program is an integrated suite of products, services, and business practices that provide a common infrastructure supporting the National Airspace System (NAS) requirements for voice, data, and video services; improve visibility into network operations, service delivery status, and cost of services; and integrate new technologies as soon as they emerge. Reference: NSTAC Financial Services Task Force Report on Network Resilience, [http://www.ncs.gov/nstac/nstac\\_publications.html](http://www.ncs.gov/nstac/nstac_publications.html).



networks and services are supported by a number of National Security and Emergency Preparedness (NS/EP) programs available from the Department of Homeland Security (DHS) National Communications System (NCS).<sup>17</sup>

The main function of ARTCCs is to control air traffic in surrounding regions. Regions are divided into sections and aircraft are monitored from section to section before being handed off to another ARTCC or to an airport approach control center. The process is highly computerized with quadruple computer redundancy and redundant power and internal communication systems.

The ARTCCs are composed, in part, of computer networks based on commercial components. Similar components have been EMP tested and have manifested latching upsets (requiring manual intervention to restore function) beginning in the 4 kV/m peak field range. Permanent damage has been observed in the 8 kV/m range but is more prevalent above 15 kV/m. Based on similarity, it is anticipated that ARTCCs will begin to manifest loss of function following EMP exposure to peak fields as low as 4 kV/m; but functions will not be seriously degraded unless exposed to peak fields in excess of 15 kV/m.

A large number of radars have overlapping coverage. Failure of a single radar will not significantly impact air traffic control capability. Simultaneous failure of multiple radars, as could happen in an EMP attack, could shutdown all air traffic control in the affected region, and possibly nationwide, thereby making it more difficult to assure safe landings. In this case, emphasis for safe landings would shift to aircraft crew and airport towers.

Power to all critical components of the FAA system is backed by fuel generator power, and in some instances, uninterrupted through temporary use of large UPSs. Visual flight operations will be in the forefront for collision avoidance and landing. Many aircraft will land at airports other than originally intended, as was the case after the 9/11 terrorist attacks. Significant challenges arise for safe landing in conditions of low visibility in the absence of navigation and landing aids at night and during adverse weather.

There are redundant radio communications with aircraft and redundant telephone and microwave communications between air traffic control regions and airport towers. If communications are lost, responsibility for safe landings will revert solely to the aircraft crews.

If the FAA air traffic control system is damaged by exposure to EMP environments, its reconstitution would take time. The FAA does not have sufficient staff or spare equipment to do a mass rapid repair of essential equipment. The FAA collection of radar, communication, navigation, and weather instruments spans 40 years. It includes components from multiple vendors that are connected using a variety of wire, wireless, and fiber links. Some equipment has lightning and electromagnetic interference protection. Accordingly, configuration control is difficult. It would take days to a month or more to bring various components of the control system back online, starting with communications, followed with navigation aids. As the control system rebuilds, there is likely to be significant reduction in air traffic, with constraints to increase intervals for departures, landings, and spacing of aircraft en route. Moreover, the capability to restore the air traffic control system is dependent on availability of services from other infrastructures. In the event these services are compromised by an EMP attack, the air traffic control restoration times will be extended.

---

<sup>17</sup> Telecommunications Service Priority (TSP), <http://tsp.ncs.gov>.

## Recommendations

Specific actions for each transportation infrastructure follow.

### ***Railroads***

Railroad operations are designed to continue under stressed conditions. Backup power and provisioning is provided for operations to continue for days or even weeks at reduced capacity. However, some existing emergency procedures, such as transferring operations to backup sites, rely on significant warning time, such as may be received in a weather forecast before a hurricane. An EMP attack may occur without warning, thereby compromising the viability of available emergency procedures. Our recommendations are directed toward mitigating this and other potential weaknesses. DHS should:

- ◆ Heighten railroad officials' awareness of the possibility of EMP attack, occurring without warning, that would produce wide-area, long-term disruption and damage to electronic systems.
- ◆ Perform a test-based EMP assessment of railroad traffic control centers. Develop and implement an EMP survivability plan that minimizes the potential for adverse long-term EMP effects. The emphasis of this effort should be on electronic control and telecommunication systems.
- ◆ Perform an EMP vulnerability assessment of current vintage railroad engines.
- ◆ Develop and implement an EMP survivability plan, if needed.

### ***Trucking and Automobiles***

Emphasizing prevention and emergency clearing of traffic congestion, DHS should coordinate a government and private sector program to:

- ◆ Initiate an outreach program to educate state and local authorities and traffic engineers on EMP effects and the expectation of traffic signal malfunctions, vehicle disruption and damage, and consequent traffic congestion.
- ◆ Work with municipalities to formulate recovery plans, including emergency clearing of traffic congestion and provisioning spare controller cards that could be used to repair controller boxes.
- ◆ Sponsor the development of economical protection modules—preliminary results for which are already available from Commission-sponsored research—that could be retrofitted into existing traffic signal controller boxes and installed in new controller boxes during manufacturing.

### ***Maritime Shipping***

The essential port operations to be safeguarded are ship traffic control, cargo loading and unloading, and cargo storage and movement (incoming and outgoing). Ship traffic control is provided by the Coast Guard, which has robust backup procedures in place. Cargo storage and movement is covered by other transportation infrastructure recommendations. Therefore, focusing on cargo operations in this area, DHS should coordinate a government and private sector program to:

- ◆ Heighten port officials' awareness of the wide geographic coverage of EMP fields, the risk caused by loss of commercial power for protracted time intervals, and the need to evaluate the practicality of providing emergency generators for at least some portion of port and cargo operations.
- ◆ Assess the vulnerability of electric-powered loading and unloading equipment.

- ◆ Review the electromagnetic protection already in place for lightning and require augmentation of this protection to provide significant EMP robustness.
- ◆ Coordinate findings with the real-time repair crews to ensure they are aware of the potential for EMP damage, and, based on the assessment results, recommend spares provisions so that repairs can be made in a timely manner.
- ◆ Assess port data centers for the potential of loss of data in electronic media.
- ◆ Provide useful measures of protection against EMP causing loss of function data.
- ◆ Provide protected off-line spare parts and computers sufficient for minimum essential operations.
- ◆ Provide survivable radio and satellite communication capabilities for the Coast Guard and the nation's ports.

### ***Commercial Aviation***

In priority order, commercial aviation must be assured that airplanes caught in the air during an EMP attack can land safely, that critical recovery assets are protected, and that contingency plans for an extended no-fly period are developed. Thus, DHS, working with the Department of Transportation, should:

- ◆ Coordinate a government program in cooperation with the FAA to perform an operational assessment of the air traffic control system to identify and provide the minimal essential capabilities necessary to return the air traffic control capability to at least a basic level of service after an EMP attack.
- ◆ Based on the results of this operational assessment, develop tactics for protection, operational workarounds, spares provisioning, and repairs to return to a minimum-essential service level.

### ***All Transportation Sectors***

- ◆ DHS should incorporate EMP effects assessment in existing risk assessment protocols.

## Chapter 7. Food Infrastructure

### Introduction

A high-altitude electromagnetic pulse (EMP) attack can damage or disrupt the infrastructure that supplies food to the population of the United States. Food is vital for individual health and welfare and the functioning of the economy.

### Dependence of Food on Other Infrastructures

The food infrastructure depends critically for its operation on electricity and on other infrastructures that rely on electricity. An EMP attack could disrupt, damage, or destroy these systems, which are necessary in making, processing, and distributing food.

Agriculture for growing all major crops requires large quantities of water, usually supplied through irrigation or other artificial means using electric pumps, valves, and other machinery to draw or redirect water from aquifers, aqueducts, and reservoirs. Tractors and farm equipment for plowing, planting, tending, and harvesting crops have electronic ignition systems and other electronic components. Farm machinery runs on gasoline and petroleum products supplied by pipelines, pumps, and transportation systems that run on electricity or that depend on electronic components. Fertilizers and insecticides that make possible high yields from croplands are manufactured and applied through means containing various electronic components. Egg farms and poultry farms typically sustain dense populations in carefully controlled environments using automated feeding, watering, and air conditioning systems. Dairy farms rely heavily on electrically powered equipment for milking cattle and for making other dairy products. These are just a few examples of how modern food production depends on electrical equipment and the electric power grid, which are both potentially vulnerable to EMP.

Food processing also requires electricity. Cleaning, sorting, packaging, and canning of all kinds of agricultural products are performed by electrically powered machinery. Butchering, cleaning, and packaging of poultry, pork, beef, fish, and other meat products also are typically automated operations, done on electrically driven processing lines. An EMP attack could render inoperable the electric equipment and automated systems that are ubiquitous and indispensable to the modern food processing industry.

Food distribution also depends heavily on electricity. Vast quantities of vegetables, fruits, and meats are stored in warehouses, where they are preserved by refrigeration systems, ready for distribution to supermarkets. Refrigerated trucks and trains are the main means of moving perishable foods to market; therefore, food distribution also has a critical dependence on the infrastructure for ground transportation. Ground transportation relies on the electric grid that powers electric trains; runs pipelines and pumping stations for gasoline; and powers signal lights, street lights, switching tracks, and other electronic equipment for regulating traffic on roads and rails.

Because supermarkets typically carry only enough food to supply local populations for 1 to 3 days and need to be resupplied continually from regional warehouses, transportation and distribution of food to supermarkets may be the weakest link in the food infrastructure in the event of an EMP attack. The trend toward modernization of supermarkets may exacerbate this problem by deliberately reducing the amount of food stored in supermarkets and regional warehouses in favor of a new just-in-time food distribution system. The new system relies on electronic databases to keep track of supermarket inventories so that they can be replaced with fresh foods exactly when needed, greatly reducing the need for large stocks of warehoused foods.

---

The electric power grid, on which the food infrastructure depends, has been component-tested and evaluated against EMP and is known to be vulnerable. Moreover, power grid blackouts induced by storms and mechanical failures on numerous occasions have caused massive failure of supermarket refrigeration systems and impeded transportation and distribution of food, resulting in spoilage of all perishable foods and causing food shortages lasting days or sometimes weeks. These storm- and accident-induced blackouts of the power grid are not likely to have consequences for the food infrastructure as severe or as geographically widespread as an EMP attack would.

In the face of some natural disasters like Hurricane Andrew in 1992, federal, state, and local emergency services combined have sometimes been hard pressed to provide the endangered population with food. Fortunately, there are few known instances of actual food starvation fatalities in the United States. In such localized emergencies as Hurricane Andrew, neighboring areas of the disaster area are usually able to provide needed emergency services (e.g., food, water, fire, and medical) in a timely fashion.

In the case of Hurricane Andrew, for example, although the area of the damage was relatively small, the level of damage was extraordinary and many people were affected. Consequently, emergency services were brought in, not just from neighboring states, but from many distant states. For example, electric transformers were brought in from other states to help rebuild the local power grid. The net result was a nationwide shortage of transformers for 1 year until replacements could be procured from overseas suppliers, who needed 6 months to build new transformers.

Hurricane Katrina, one of the greatest natural disasters ever to strike the United States, afflicted a much larger area than Andrew. Consequently, the ability to provide food and other emergency aid was a much greater challenge. The area disrupted by Hurricane Katrina is comparable to what can be expected from a small EMP attack.

Recent federal efforts to better protect the food infrastructure from terrorist attack tend to focus on preventing small-scale disruption of the food infrastructure, such as would result from terrorists poisoning some portion of the food supply. Yet an EMP attack potentially could disrupt or collapse the food infrastructure over a large region encompassing many cities for a protracted period of weeks, months, or even longer. Widespread damage of the infrastructures would impede the ability of undamaged fringe areas to aid in recovery. Therefore, it is highly possible that the recovery time would be very slow and the amount of human suffering great, including loss of life.

### **Making, Processing, and Distributing Food**

The United States is a food superpower. It leads the world in production of the 10 major crops, nine of which are food sources: corn, soybeans, wheat, upland cotton, sorghum, barley, oats, rice, sunflowers, and peanuts. The United States is also a world leader in the production of meats, poultry, and fish. Of the world's 183 nations, only a few are net exporters of grain. The United States, Canada, Australia, and Argentina supply over 80 percent of the net cereal grains exported worldwide—the United States alone providing more than half.

These U.S. exports go far toward alleviating hunger and preserving political stability in many nations that lack the resources to feed their own populations. While most Americans tend to take for granted the quantity and high quality of food available to them on a daily basis, most other countries of the world regard the United States' food infrastructure as an enviable economic miracle.



In contrast to the United States, many of the world's nations struggle to meet the food demands of their populations, even though in some cases those populations are living near or below a subsistence level. Most of the world's 183 nations, to some degree, are dependent on food imports. Even among the advanced nations, the United States is exceptional for the quantity and quality of its food production.

U.S. consumers are supplied largely from domestically produced food. In 2002, according to data from the U.S. Department of Agriculture (USDA), some 2.1 million U.S. farms sold about \$192 billion in crops and livestock. U.S. farms have 455 million acres under cultivation for crop production. Another 580 million acres in the United States are pasture and range land that support raising livestock.

Raw agricultural commodities are converted to intermediate foodstuffs and edible foods by some 29,000 processing plants located throughout the United States, according to the Census of Manufacturers. These plants employ about 1.7 million workers, which is approximately 10 percent of all U.S. manufacturing employment and just over 1 percent of all U.S. employment. Most plants are small, but larger establishments account for the major portion of shipments. The 20 largest firms in food manufacturing account for about 35 percent of shipments, while in beverage manufacturing, the 20 largest firms account for 66 percent of shipments. The largest 50 firms account for 51 percent of food shipments and 74 percent of beverage shipments.

Food is supplied to consumers by approximately 225,000 food stores, as well as by farmers markets and pick-your-own farms. Away-from-home food service is provided by approximately 850,000 establishments, including restaurants, cafeterias, fast food outlets, caterers, and others.

To illustrate how the U.S. food infrastructure works in making, processing, and distributing food from farm to market, here is a concrete example:

Washington State is the foremost apple producer in the United States, with more than \$850 million in annual sales and 225,000 acres of orchards, mostly in the Cascade Mountains. A major supermarket chain contracts through a cooperative of medium-sized apple growers in the Spokane area to grow apples.

In the course of the growing season, the Spokane apple farmers use a wide array of farm machinery to tend their trees and to apply fertilizers and pesticides. During the harvest season, Washington farmers employ 35,000 to 45,000 pickers to harvest their apple crops. Hand-picked apples are loaded onto flatbed trucks and shipped to processing firms belonging to or under contract with the chain. Apples are processed on an electrically driven assembly line that uses a variety of electromechanical devices to clean fruit of dirt and pesticide residue, sort and grade apples according to size and quality, wax the fruit, and package it into 40-pound cartons.

If the apples are not to be sent to market immediately, they can be stored for up to 8 months in giant refrigerators. The chain arranges for a shipment of apples to its Maryland distribution center, located in Upper Marlboro, which services its stores in the Washington, D.C., area. A trucking company is contracted for the 4-to-5 day shipment of apples to the East Coast using a refrigerated truck. The apples are offloaded at the Upper Marlboro regional distribution center, which makes daily deliveries to the chain's stores. A refrigerated truck delivers apples to a Washington, D.C., supermarket. Local residents purchase the apples.

This example of how the food infrastructure works for apples from grower to consumer generally is the same for most foods, with differences in detail. One important difference is that apples, compared to many other crops, are among those most dependent on manual labor and least dependent on machinery. Yet, clearly the food infrastructure, even for the apple, depends heavily on assembly lines, mechanical sorters and cleaners, refrigerators, and vehicles that, directly or indirectly, cannot operate without electricity.

### **Vulnerability to EMP**

An EMP attack could damage or destroy some fraction of the myriad electronic systems, ubiquitous throughout the food infrastructure, that are essential to making, processing, and distributing food. Growing crops and raising livestock require vast quantities of water delivered by a water infrastructure that is largely electrically powered. Tractors, planters, harvesters, and other farm equipment are fueled by petroleum products supplied by pipelines, pumps, and transportation systems that run on electricity. Fertilizers, insecticides, and feeds that make possible high yields from crops and livestock are manufactured by plants requiring electric power.

Food processing—cleaning, sorting, packaging, and canning of all kinds of agricultural and meat products—is typically an automated operation, performed on assembly lines by electrically powered machinery.

Food distribution also depends on electricity. Refrigerated warehouses make possible the long-term storage of vast quantities of vegetables, fruits, and meats. Road and rail transportation depend on the electric grid that powers electric trains, runs pipelines and gas pumps, and powers the apparatus for regulating traffic on roads and rails.

Because the United States is a food superpower with relatively few farmers, technology is no longer merely a convenience—it is indispensable to the farmers who must feed the nation's population and much of the rest of the world.

In 1900, 39 percent of the U.S. population (about 30 million people) lived on farms; today that percentage has plummeted to less than 2 percent (only about 4.5 million people). The United States no longer has a large labor force skilled in farming that could be mobilized in an emergency. The transformation of the United States from a nation of farmers to a nation in which less than 2 percent of the population is able to feed the other 98 percent is made possible only by technology. Crippling that technology would be injurious to the food infrastructure with its security depending on the characteristics of an EMP attack.

The dependency of the U.S. food infrastructure on technology is much greater than implied by the reduction in the percentage of farmers from 39 percent in 1900 to less than 2 percent of the population today. Since 1900, the number of acres under cultivation in the United States has increased by only 6 percent, yet the U.S. population has grown from about 76 million people in 1900 to 300 million today. In order for a considerably reduced number of U.S. farmers to feed a U.S. national population that has grown roughly four-fold from approximately the same acreage that was under cultivation in 1900, the productivity of the modern U.S. farmer has had to increase by more than 50-fold. Technology, in the form of machines, modern fertilizers and pesticides, and high-yield crops and feeds, is the key to this revolution in food production. An attack that neutralized farming technology would depress U.S. food production.

The food processing industry is an obvious technological chokepoint in the U.S. food infrastructure. Food processing of vegetables, fruits, and all kind of meats is a highly automated, assembly-line operation, largely driven by electric power. An EMP attack that damages this machinery or blacks out the power grid would stop food processing. The work force in the food processing industry is sized and trained to run a largely automated system. In the event of an attack that stops the machines from running, personnel would not be sufficiently numerous or knowledgeable to process food the old-fashioned way, by hand. Depending on climate, most foods that are not refrigerated would begin to spoil in a few hours or days.

Finally, the distribution system is probably the most vulnerable technological chokepoint in the U.S. food infrastructure. Supermarkets typically carry only enough food to provision the local population for 1 to 3 days. Supermarkets replenish their stocks virtually on a daily basis from regional warehouses, which usually carry enough food to supply a multicounty area for about 1 month.

Regional warehouses are probably the United States' best near-term defense against a food shortage because of the enormous quantities of foodstuffs stored there. For example, one typical warehouse in New York City daily receives deliveries of food from more than 20 tractor trailers and redistributes to market more than 480,000 pounds of food. The warehouse is larger than several football fields, occupying more than 100,000 square feet. Packaged, canned, and fresh foods are stored in palletized stacks 35 feet high. Enormous refrigerators preserve vegetables, fruits, and meats and the entire facility is temperature controlled.

However, regional warehouses potentially are vulnerable to an attack that collapses the power grid and causes refrigeration and temperature controls to fail. Moreover, the large quantities of food kept in regional warehouses will do little to alleviate a crisis if it cannot be distributed to the population promptly. Distribution depends largely on trucks and a functioning transportation system. Yet storm-induced blackouts have caused widespread failure of commercial refrigeration systems and massive food spoilage.

Trends in the grocery industry toward just-in-time distribution may reduce reliance on regional warehouses and increase the vulnerability of the food infrastructure to EMP attack. Just-in-time distribution, now being adopted by some supermarket chains in California, Pennsylvania, and New Hampshire, uses automated databases and computer systems to track supermarket inventories in real time and promptly replenish food inventories, as needed, from even larger, but fewer, regional warehouses and directly from food manufacturers.

The new system promises to supply customers with fresher foods and to greatly reduce industry's reliance on large inventories of stockpiled foods at regional warehouses. As just-in-time distribution becomes the industry norm, in the event of an EMP attack, heavier reliance on computers and databases may make it easier to disrupt the management of food distribution, while decreased reliance on regional warehouses could greatly reduce the amount of food available for distribution in an emergency.

*Pulse-current injection and free-field illumination testing on a limited number of refrigerators and freezers indicate that some units will fail from low to moderate EMP levels. This testing indicates that substantial numbers of people would have to survive without benefit of refrigerated foods for an extended period, until repairs or replacement refrigerators and freezers could be obtained. Massive food spoilage at stores and regional warehouses is implied.*

### **Consequences of Food Infrastructure Failure**

An EMP attack that disrupts the food infrastructure could pose a threat to life, industrial activity, and social order. Absolute deprivation of food, on average, will greatly diminish a person's capacity for physical work within a few days. After 4 to 5 days without food, the average person will suffer from impaired judgment and have difficulty performing simple intellectual tasks. After 2 weeks without food, the average person will be virtually incapacitated. Death typically results after 1 or 2 months without food.

This timeline would not start until food stockpiles in stores and homes were depleted. Many people have several days to weeks of food stored in their homes. For example, in 1996 when a snowstorm in the Washington, D.C., area virtually paralyzed the food infrastructure for a week, the general population was forced to live off of private food larders and had sufficient stores to see them through the emergency. However, a significant number of people, those with little or no home food supply, would have to begin looking for food immediately.

Historically, even the United States' vast agricultural wealth has not always been enough to protect its people from the effects of nature and bad economic decisions. Millions of Americans knew hunger as a consequence of a drought that caused the dust bowl years (1935 to 1938) in the Western and Central Plains breadbasket, as well as by the Wall Street crash of 1929 and the Great Depression. Even today, according to the USDA, 33.6 million Americans, almost 12 percent of the national population, live in "food-insecure households." Food-insecure households, as defined by the USDA, are households that are uncertain of having or are unable to acquire enough food to meet the nutritional needs of all their members because they have insufficient money or other resources.

A natural disaster or deliberate attack that makes food less available, or more expensive, would place at least America's poor, 33.6 million people, at grave risk. They would have the least food stockpiled at home and be the first to need food supplies. A work force preoccupied with finding food would be unable to perform its normal jobs. Social order likely would decay if a food shortage were protracted. A government that cannot supply the population with enough food to preserve health and life could face anarchy.

In the event of a crisis, often merely in the event of bad weather, supermarket shelves are quickly stripped as some people begin to hoard food. Hoarding deprives government of the opportunity to ration local food supplies to ensure that all people are adequately fed in the event of a food shortage. The ability to promptly replenish supermarket food supplies becomes imperative in order to avoid mass hunger.

Blackouts of the electric grid caused by storms or accidents have destroyed food supplies. An EMP attack that damages the power grid and denies electricity to warehouses or that directly damages refrigeration and temperature control systems could destroy most of

the 30-day regional perishable food supply. Blackouts also have disrupted transportation systems and impeded the replenishment of local food supplies.

Federal, state, and local government agencies combined sometimes have had difficulty compensating for food shortages caused by storm-induced blackouts. For example:

- ◆ Hurricane Katrina in August 2005 caused a protracted blackout in New Orleans and the coastal region, destroying the food supply. Flooding, downed trees, and washed-out bridges paralyzed transportation. But the Katrina blackout by itself was sufficient to stop transportation and prevent rapid replenishment and repair of the food infrastructure because gas stations could not operate without electric power. An EMP attack could also paralyze transportation of food by rendering gas pumps inoperable, causing vehicles to fail and blacking out traffic lights, resulting in massive traffic jams. Hurricane Katrina's destruction of the food supply was a major contributing factor to the necessity of mass evacuation of New Orleans and the coastal population. Because many evacuees never returned, the protracted disruption of the food infrastructure, which lasted weeks—and in some localities months—while the electric power grid was being restored, was a major factor contributing to permanently reducing the populations of New Orleans and coastal Louisiana. Hurricane Katrina's effect on the food infrastructure is comparable to what can be expected from a small EMP attack.
- ◆ Hurricane Lili in October 2002 blacked out the power grid in coastal Louisiana, virtually collapsing the local food infrastructure. As a consequence of the blackout, food was unavailable to thousands through normal means. In south Louisiana, 30 supermarkets would not open because the blackout prevented their electric cash registers from operating. Those stores that did open were stripped of food within hours. In Abbeville, the parking lots of shopping centers became feeding stations run by churches and the state Office of Emergency Preparedness. Associated Grocers, which supplies food to supermarkets in Louisiana, Texas, and Mississippi, sent food in refrigerated trucks to the area from regional warehouses.

The food emergency was reflected in a skyrocketing demand for dry ice to preserve food stuffs during the hot weather and to preserve refrigerated foods. Local supplies of dry ice were exhausted quickly—one store selling 20,000 pounds of dry ice to hundreds of customers in 2 hours—and had to be supplemented with supplies from the Red Cross.

It is important to note that no one died from food or water deprivation during this emergency, and that the damaged area was small enough to be aided rapidly during recovery by undamaged fringe areas.

- ◆ Hurricane Floyd in September 1999 put more than 200 supermarkets out of operation in North Carolina. Protracted blackouts caused massive food spoilage despite emergency efforts taken before the storm to preserve perishable goods in freezers. Floyd blackouts also impeded replenishment of some supermarkets by inducing traffic signal failures that contributed to massive traffic jams.
- ◆ An ice storm blacked out the Washington, D.C., area in January 1999. Warm food, potentially a survival issue in the freezing winter conditions, was not available in most people's homes because electric ovens and microwaves no longer worked.

In addition, most gas-powered ovens would not work because those built since the mid-1980s have electronic ignition and cannot be lit with a match. Some resorted to cooking on camp stoves. Preserving refrigerated foods was also a concern that Pepco,



the regional power authority, helped address by giving away 120,000 pounds of dry ice, all that it had. Dry ice became a precious commodity.

- ◆ In January 1998, an ice storm caused a widespread blackout affecting parts of Ontario and Quebec in Canada, and Maine and upstate New York in the United States. The blackout threatened the food supply. According to press reports, “Food poisoning has become a real threat as embattled Montrealers, unable to get to stores, eat food that has been kept too long in refrigerators that no longer work.”

In upstate New York, the electric utility Niagara Mohawk announced that it was focusing restoration of electric power on more populated areas “so that supermarkets, gasoline stations, and hotels could reopen, and people in the more rural areas could find food and shelter.” New York State Electric and Gas helped customers get to shelters and distributed 200,000 pounds of dry ice for preserving food.

- ◆ Hurricane Andrew in August 1992 laid waste to 165 square miles in South Florida and left 3.3 million homes and businesses without electricity. Andrew’s aftermath posed an immediate threat to life in South Florida, in part because of damage to the food infrastructure. Most grocery stores had been destroyed.

Massive traffic jams, caused in part by nonfunctioning signal and street lights, prevented the surviving supermarkets from being resupplied. “More than 5,000 traffic lights are on the blink,” the press reported. “Traffic was snarled for miles. The simplest chore, indeed almost everything, seemed to take forever.”

To meet the crisis, tons of surplus food were distributed in the area. Nonetheless, two weeks after the hurricane, food was still not reaching many victims.

Andrew’s blackout of the power grid made the crisis over food, water, and shelter worse by severing communications between relief workers and victims. Without power, there was an almost complete collapse of communications—no telephones, radio, or television. Consequently, many people were unaware of relief efforts or of where to go for help. Had Hurricane Andrew damaged a larger area, it is likely that undamaged fringe areas would have been less capable of coming to the rescue, resulting in a significant loss of life.

Storm-induced blackouts provide some basis for extrapolating the greater destructive effects on food infrastructure likely from an EMP attack. An EMP attack is likely to damage electric power grids and other systems over a much wider geographic area than blackouts caused by storms; therefore, recovery from an EMP attack probably would take longer. An EMP attack also could directly damage some electronic systems, including refrigeration systems and vehicles, which normally would not be damaged by a blackout. Compared to blackouts, an EMP attack could inflict damage over a wider geographic area and damage a much wider array of equipment; consequently, recovery of the food infrastructure from EMP is likely to be much more complicated and more protracted.

Federal, state, and local agencies combined would find it difficult to cope immediately or even over a protracted period of days or weeks following an EMP attack that causes the food infrastructure to fail across a broad geographic area encompassing one or more states. Infrastructure failure at the level of food distribution because of disruption of the transportation system, as is likely during an EMP attack, could bring on food shortages affecting the general population in as little as 24 hours.

Massive traffic jams are most likely in large cities, the very areas where rapid replenishment of the food supply at hundreds of supermarkets will be needed most urgently. Significantly, recent famines in the developing world have occurred, despite massive relief efforts by the international community, in large part because food relief could not reach victim populations through their underdeveloped transportation infrastructure. An EMP attack could, in effect, temporarily create in the United States the technological conditions in the food and transportation infrastructures that have resulted in developing world famines.

## Recommendations

Current planning, as reflected in the President's National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, the Public Health, Security, and Bioterrorism Preparedness and Response Act of 2002 (the Bioterrorism Act), and Federal Emergency Management Agency (FEMA) planning documents, all appear to assume relatively small-scale threats to the food infrastructure. Most concern is focused on terrorists' poisoning or infecting a small portion of the food supply to cause mass panic and public fear about the safety of all food. The FEMA Federal Response Plan for a food shortage assumes a disaster effecting about 10,000 people: "On the fringes of the geographic areas affected will be schools and small institutions having large inventories estimated to be sufficient to feed up to 10,000 people for 3 days and supply their fluid needs for 1 day."<sup>1</sup> Yet an EMP attack could so damage the food infrastructure that millions of people would be at risk. Recommendations to address this risk include the following:

- ◆ Relevant federal agencies, including the Department of Homeland Security and the USDA, should supplement their plans to meet food emergencies by drawing on federal food stockpiles.
- ◆ Federal food stockpiles should be sized to meet a possible large-scale food shortage in the event of massive disruption of the national food infrastructure from an EMP attack or other causes.
- ◆ The Federal Government should examine useful lessons learned from reviewing earlier plans and programs, such as those during the early Cold War years, when the Federal Government planned and prepared for food shortages on a large scale.
- ◆ The Federal Government should plan to locate, preserve, deliver, distribute, and ration existing stockpiles of processed and unprocessed food, including food stockpiles by the USDA and other government agencies, which will be an important component of maintaining the food supply.
- ◆ The Federal Government should make it a priority to plan to protect, deliver, and ration food from regional warehouses, under conditions in which an EMP attack has disrupted the power, transportation, and other infrastructures for a protracted period.
- ◆ The Federal Government should make plans to process and deliver private and government grain stockpiles to significantly supplement the processed food stored in regional warehouses. According to the USDA's National Agricultural Statistical Service, total private grain stockpiles in the United States amount to more than 255 million metric tons. Federal grain stockpiles held by the Commodity Credit Corporation exceed 1.7

---

<sup>1</sup> FEMA, Response and Recovery, Emergency Support Function No. 11 Food Annex, <http://www.au.af.mil/au/awc/awcgate/frp/frpesf11.htm>.

million metric tons, with 1.6 million metric tons of that amount dedicated to the Bill Emerson Humanitarian Trust for overseas emergency.

- ◆ The Federal Government should increase food stockpiles if existing stockpiles of food appear to be inadequate.
- ◆ Contingency plans also should be made to provide significant levels of personnel and technical support to speed the recovery of agriculture and food production from an EMP attack.

Presidential initiatives have designated the Department of Homeland Security as the lead agency responsible for the security of the food infrastructure, overseeing and working with the USDA. Currently, under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (the *Stafford Act*) the President “is authorized and directed to assure that adequate stocks of food will be ready and conveniently available for emergency mass feeding or distribution” in the United States.<sup>2</sup> However, in practice, the *Stafford Act* has been used to authorize purchasing food from private sources and issuing food coupons to be used in supermarkets in order to meet food shortages.

In some particularly dire emergencies, as during Hurricane Katrina and Hurricane Andrew, when private sector food resources were destroyed or inadequate to meet the crisis, the Federal Government has resorted to federal surplus foods. Many Andrew victims were saved from hunger by Meals Ready to Eat (MRE). But the Federal Government was surprised by Andrew, and the resort to MREs and surplus food stockpiles was a poorly planned act of desperation that came late in the crisis. Recommendations to achieve this initiative include the following:

- ◆ The Federal Government should consider one readily available option, which is to grow the food stockpile to include the MREs.
- ◆ Plans should include timely distribution of mass quantities of food, which is likely to be crucial during a shortage.
- ◆ The *Stafford Act* should be amended to provide for plans to locate, protect, and distribute existing private and government stockpiles of food and to provide plans for distributing existing food stockpiles to the general population in the event of a national emergency.

---

<sup>2</sup> Appendix B, Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288, as amended (as of September 1, 1999), p. B-43, <http://www.fema.gov/pdf/government/grant/pa/pagappb.pdf>.

## Chapter 8. Water Infrastructure

### Introduction

Water and its system of supply is a vital infrastructure. High-altitude electromagnetic pulse (EMP) can damage or disrupt the infrastructure that supplies water to the population, agriculture, and industry of the United States (U.S.).

The water infrastructure depends for its operation on electricity. To the extent possible, aqueducts, tunnels, pipelines, and other water delivery systems are designed to rely on gravity. However, since the invention and proliferation of the electric water pump early in the last century, urban growth, planning, and architecture have been liberated from dependence on gravity-fed water systems. By making water move uphill, the gravity pump has made possible the construction and growth of cities and towns in locations that, in previous centuries, would have been impossible. Skyscrapers and high-rise buildings, which would be impractical if dependent on a gravity-fed water system, have been made possible by the electric pump.

Electrically driven pumps, valves, filters, and a wide variety of other electrical machinery are indispensable for the purification of water for drinking and industrial purposes and for delivering water to consumers. An EMP attack could degrade or damage these systems, affecting the delivery of water to a very large geographic region.

Electrical machinery is also indispensable to the removal and treatment of wastewater. An EMP attack that degraded the processes for removing and treating wastewater could quickly cause public health problems over a wide area.

Supervisory and Control Data Acquisition Systems (SCADA) are critical to the running and management of the infrastructure for delivery of pure water for drinking, for industry, and for the removal and treatment of wastewater. SCADAs enable centralized control and diagnostics of system problems and failures and have made possible the regulation and repair of the water infrastructure with a small fraction of the work force required in earlier days. As discussed in greater detail in Chapter 1, an EMP attack could damage or destroy SCADAs, making it difficult to manage the water infrastructure and to identify and diagnose system problems and overwhelming the small work force with systemwide electrical failures.

The electric power grid provides the energy that runs the water infrastructure. An EMP attack that disrupts or collapses the power grid would disrupt or stop the operation of the SCADAs and electrical machinery in the water infrastructure. Some water systems have emergency power generators, which could provide continued — albeit greatly reduced — water supply and wastewater operations for a short time.

Little analysis has been conducted of the potential vulnerability of the water infrastructure to EMP attack. However, SCADAs supporting the water infrastructure are known not to have been hardened, or in most cases even tested, against the effects of an EMP attack.

The electric power grid, on which the water infrastructure is critically dependent, is known to be vulnerable to feasible levels of EMP. Moreover, blackouts of the power grid induced by storms and mechanical failures are known to have disrupted the water infrastructure on numerous occasions. These storm- and accident-induced blackouts of the power grid are not likely to be as severe or as geographically widespread in their consequences for the water infrastructure as would an EMP attack.

Federal, state, and local emergency services, faced with the failure of the water infrastructure in a single large city, would be hard pressed to provide the population with the minimum water requirements necessary to sustain life over a time frame longer than a few days. They could not provide, on an extended emergency basis, the water requirements and services, including waste removal, necessary to sustain normal habitation and industrial production in a single large city; however, an EMP attack could disrupt the water infrastructure over a large geographic area encompassing many cities for a protracted period of weeks or even months.

### **The Water Works**

Water for consumption and sanitation is taken for granted by virtually everyone in the United States. Yet, the infrastructure for supplying pure water to the U.S. population and industry and for removing and treating wastewater, compared to other infrastructures, took longer to build and arguably is the most important of all infrastructures for the sustenance of human life.

One of the most important differences between developed and underdeveloped nations is the availability of pure water. An estimated 1.3 billion people in the developing world, nearly one-quarter of the global population, lack access to safe drinking water and even more, approximately 1.8 billion, lack water for sanitation. Consequently, diseases related to impure water flourish in many underdeveloped nations, taking a devastating toll on health and longevity. Economic development in many developing world nations is impeded by the absence of an adequate water supply to support industry. Indeed, in some countries, a major obstacle to development is simply the fact that the labor force has no alternative but to spend much of its time transporting water for drinking and other domestic uses from distant and often contaminated sources.

In contrast to the water scarcity that impedes development in much of the developing world, the United States enjoys a healthy and growing population and economic prosperity supported by the efficient distribution and utilization of its abundant water resources. Freshwater consumption for all purposes averages about 1,300 gallons per capita per day in the United States. Irrigation and cooling account for about 80 percent of all consumption, and, in the 17 western states, irrigation alone accounts for more than 80 percent of water consumption. On average, some 100 gallons per person per day (200 gallons per person per day in the southwest) are consumed for domestic purposes such as drinking, bathing, preparing food, washing clothes and dishes, flushing toilets, washing cars, and watering lawns and gardens.

Drinking and cooking account for only a small fraction of the water consumed; however, because in most cases a single water source must serve all purposes, all water consumed, regardless of the purpose, must meet the standards for drinking water purity, as prescribed by law.

Supporting this demand for enormous quantities of high-quality water is a vast infrastructure that includes more than 75,000 dams and reservoirs; thousands of miles of pipes, aqueducts, and water distribution and sewer lines; 168,000 drinking water treatment facilities; and 19,500 wastewater treatment facilities.

A fairly small number of large drinking water and wastewater utilities located primarily in urban areas (about 15 percent of the systems) provide water services to more than 75 percent of the U.S. population.



There is no single organization or system controlling the entire water infrastructure of the United States. Rather, more than 100,000 utilities and private owners manage the national water infrastructure. However, because water utilities provide similar services and must meet similar standards, they all operate in much the same way.

Water supplies require collection, treatment, storage, and distribution. Surface water such as reservoirs, lakes, and rivers generally provides water for cities. Wells tapping underground aquifers often supply rural areas and the southwestern states. Homeowners with private wells typically drink the water directly, because the subsurface water has been filtered over many years within the natural underground sedimentation. Water treatment plants are designed to provide an uninterrupted water supply that raises the purity of surface water and aquifers to drinking standards. A typical municipal water treatment plant purifies water through several steps: filtration, coagulation, flocculation, sedimentation, and disinfection.

Filtration by utilities passes raw water first through coarse filters to remove sticks, leaves, and other large debris. Finer filtration passes water through layers of sand and other granular material to remove silt and microorganisms. This stage of treatment imitates the natural filtration of water as it moves through the ground. This entire process is accomplished through low-lift pumps and mechanically cleaned bar screens and fine screens.

Coagulation is the process of removing colloidal impurities, finely suspended particles, from the filtered water. A coagulant, such as aluminum sulfate, is thoroughly mixed into water containing colloidal particles. Aluminum sulfate not only will coagulate and remove colloidal particles, but also will react with calcium hydroxide in the water, forming aluminum hydroxide, which can be removed through further filtration or sedimentation.

Flocculation immediately follows the coagulation process to remove the finest particles that would never settle out naturally. The velocity of the water is reduced and a gentle mixing action is used to allow formation of insoluble salts, colloidal particles, and other remaining suspended matter into a “floc” particle. The colloids and the coagulants mix with each other to form a large neutral floc particle that will settle out during sedimentation.

Sedimentation involves moving the water to large tanks to allow the floc to settle to the bottom of the tank. Sedimentation basins or clarifiers are usually the largest tanks in the treatment process. About 1 pound of sludge is created for every pound of chemical added to the water for coagulation and flocculation. The sludge must be removed and disposed of and filters and screens must be backwashed regularly.

Disinfection uses chemicals to kill any microorganisms that may have survived the filtration process. Chlorine is the most common disinfectant. When chlorine combines with organic material, such as dead leaves, it produces potentially dangerous trihalomethanes (THM). Large water treatment plants in major cities often undertake an additional purification step that reduces the level of THMs. Ozone oxidation and ultraviolet light are other disinfectant processes that are sometimes used instead of or in addition to chlorine. Fluoride also may be added because of its ability to retard tooth decay. Groundwater is often aerated by bubbling air through the water or by spraying to oxidize dissolved iron and manganese and to remove odors caused by hydrogen sulfide.

Treated water is delivered by high-lift pumps to the distribution system, usually through pipelines pressurized to 40 to 80 psi, to consumers. These pumps help to maintain water levels in storage reservoirs. Gravity flow, whenever possible, is the preferred method for delivering water. However, most water must be delivered by means of electric pumps. High-pressure pumps at the treatment plant deliver water to various zones within a water district to a booster pump or series of booster pumps that completes delivery to the consumer. High-rise buildings typically are serviced by individual booster pumps with enough pressure to provide water to rooftop reservoirs for consumption by upper floors and to provide water for firefighting.

Many of the same processes used in purification of drinking water also are used in treatment of wastewater, suitably modified for the removal of the greater amounts of material found in sewage. Sewage provides an ideal environment for a vast array of microbes, primarily bacteria, plus some viruses and protozoa. In fact, wastewater processing relies on benign microorganisms in the purification process. Sewage may also contain pathogens from the excreta of people with infectious diseases that can be transmitted by contaminated water. Waterborne diseases, while seldom a problem now in developed nations, are still a threat in developing countries where treated water is not available for public use.

Contaminants are generally removed from wastewater physically, biologically, and chemically. First, rags, sticks, and large solids are removed by coarse screens to protect the pumps. Then grit, the material that wears out equipment, is settled out in grit tanks or chambers. At this point, most of the small solids are still in suspension and can be removed and concentrated in the primary gravity settling tanks. The concentrated solids, called raw sludge, are pumped to an anaerobic digester for biological decomposition. The clarified effluent then flows to secondary treatment units for biological oxidation where the dissolved and colloidal matter in wastewater provides nutrients for microorganisms. A final gravity settling tank is used to remove microorganisms. This concentrated biological sludge is removed and returned to the anaerobic digester. Chemical disinfection, usually employing chlorine, is the last stage in the treatment of wastewater before it is discharged.

### **Vulnerability to EMP**

The water infrastructure is a vast machine, powered partly by gravity but mostly by electricity. Electrically driven pumps, valves, filters, and a wide variety of other machinery and control mechanisms purify and deliver water to consumers and remove wastewater. An EMP attack could damage or destroy these systems, cutting off the water supply or poisoning the water supply with chemicals and pathogens from wastewater. For example:

- ◆ Total organic carbon (TOC) analyzers detect the levels of pollutants and pathogens in water. Determining water quality and the kind of purification treatment necessary depends on these sensors.
- ◆ Mechanical screens, filters, collector chains, skimmers, and backwash systems remove sludge and other solid wastes. Failure of these systems would pollute the water and quickly clog the pumps.
- ◆ SCADA systems enable remote control and instantaneous correction of potential problems with water quality, delivery, and wastewater removal and treatment. This process allows most water utilities to be nearly autonomous in operation, using a minimum

number of personnel. In an emergency, such as an electrical blackout, some subsystems have been or could easily be modified for workarounds. For example, many valves have a manual bypass mode, and some water plants have emergency power generators. However, the efficiencies made possible by SCADAs have reduced the available number of trained personnel probably below the levels required for protracted manual operation of water treatment facilities. The failure of SCADAs would greatly impede all operations.

- ◆ High-lift and low-lift pumps are ubiquitous throughout the infrastructure for purifying and delivering water and removing wastewater. Water cannot be purified or delivered, nor sewage removed and treated, if these systems are damaged or destroyed.
- ◆ Paddle flocculators and other types of mixers are the primary means of chlorination and other chemical purification. If these systems cease functioning, water cannot be purified and likely would remain hazardous.

All of these systems depend on the electric grid for power. Large water treatment plants consume so much electricity, in some cases about 100 megawatts, that backup generators are impractical. For reliability, water treatment plants typically draw electricity from two local power plants. An EMP attack that collapses the electric power grid will also collapse the water infrastructure.

### **Consequences of Water Infrastructure Failure**

By disrupting the water infrastructure, an EMP attack could pose a major threat to life, industrial activity, and social order. Denial of water can cause death in 3 to 4 days, depending on the climate and level of activity.

Stores typically stock enough consumable liquids to supply the normal demands of the local population for 1 to 3 days, although the demand for water and other consumable liquids would greatly increase if tap water were no longer available. Local water supplies would quickly disappear. Resupplying local stores with water would be difficult in the aftermath of an EMP attack that disrupts transportation systems, a likely condition if all critical infrastructures were disrupted.

People are likely to resort to drinking from lakes, streams, ponds, and other sources of surface water. Most surface water, especially in urban areas, is contaminated with wastes and pathogens and could cause serious illness if consumed. If water treatment and sewage plants cease operating, the concentration of wastes in surface water will certainly increase dramatically and make the risks of consuming surface water more hazardous.

One possible consequence of the failure of water treatment and sewage plants could be the release of sludge and other concentrated wastes and pathogens. Typical industrial wastes include cyanide, arsenic, mercury, cadmium, and other toxic chemicals.

Boiling water for purification would be difficult in the absence of electricity. Even most modern gas stoves require electricity for ignition and cannot be lighted by match. In any event, gas also may not be available to light the stoves (see Chapter 5). Boiling could be accomplished by open fires, fueled by wood or other flammables. Other possible mitigators are hand-held pump filters, water purification kits, iodine tablets, or a few drops of household bleach.

A prolonged water shortage may quickly lead to serious consequences. People preoccupied with finding or producing enough drinking water to sustain life would be unavailable to work at normal jobs. Most industrial processes require large quantities of water and would cease if the water infrastructure were to fail.

---

Demoralization and deterioration of social order can be expected to deepen if a water shortage is protracted. Anarchy will certainly loom if government cannot supply the population with enough water to preserve health and life.

The many homeowners with private wells also would face similar problems. There would be fewer workarounds to get their pumps operating again, if the pump controller is damaged or inoperable. Even if power is restored, it is unlikely the average homeowner would be technically competent to bypass a failed pump controller and figure out how to power the pump with bypass power lines.

The first priority would be meeting personal water needs. Federal, state, and local governments do not have the collective capability, if the water infrastructure fails over a large area, to supply enough water to the civilian population to preserve life.

Storm-induced blackouts of the electric grid have demonstrated that, in the absence of electric power, the water infrastructure will fail. Storm-induced blackouts have also demonstrated that, even in the face of merely local and small-scale failure of the water infrastructure, the combined efforts of government agencies at all levels are hard pressed to help. For example:

- ◆ Hurricane Katrina in August 2005 collapsed the water infrastructure in New Orleans and coastal Louisiana. The Katrina-induced blackout stopped the vast machinery for purifying and delivering water to the population. Water supplies were contaminated. The National Guard, among other resources, had to be mobilized to rush water and mobile water purification systems to the afflicted region. The water crisis—which was protracted because the blackout was protracted, the electric power grid requiring weeks and in some places months to repair—was a major contributing factor to the mass evacuation of the regional population. Once evacuated, many never returned. Thus the loss of water resources was a significant factor contributing to permanently reducing the population in the region. The effects of Hurricane Katrina on the water infrastructure are comparable to what can be expected from a small EMP attack.
- ◆ Hurricane Lili in October 2002 blacked out the power grid in coastal Louisiana. With no electricity, water pumps no longer worked, depriving the population of running water. Local bottled water supplies were quickly exhausted. Federal and state authorities resorted to using roadside parking lots and tanker trucks as water distribution centers.
- ◆ In September 1999, Hurricane Floyd blacked out electricity, causing water treatment and sewage plants to fail in some Virginia localities and, most notably, in Baltimore, Maryland. For several days, blackout-induced failure of Baltimore's Hampden sewage facility raised concerns about public health. With its three pumps inoperable, Hampden spilled 24 million gallons of waste into Baltimore's Jones Falls waterway and the Inner Harbor.
- ◆ An ice storm in January 1999 blacked out Canada's Ontario and Quebec provinces, causing an immediate and life-threatening emergency in Montreal's water supply, which depends on electricity for filtration and pumping. On January 9, the two water treatment plants that served 1.5 million people in the Montreal region failed, leaving the area with only enough water to last 4 to 8 hours. Government officials kept the water crisis secret, fearing public knowledge would exacerbate the crisis by water hoarding and panic. But as household water pipes went dry and reports of a water shortage spread, hoarding happened anyway and bottled water disappeared from

stores. Warnings not to drink water without boiling it proved pointless, because people had no other way of getting water and no way to boil it in the mid-winter blackout.

Montreal officials feared not only a shortage of drinking water, but also an inadequate supply of water for fighting fires. The Montreal fire department prepared to fight fires with a demolition crane instead of water, hoping that, if a building caught fire, the conflagration might be contained by demolishing surrounding structures. So desperate was the situation that provincial officials considered evacuating the city. Fortunately, Hydro-Quebec, the government's electric utility, managed to restore power to the filtration plants and restore water service before such extreme measures became necessary.

- ◆ In August 1996, a heat wave blacked out parts of the southwestern United States. Water supplies were interrupted in some regions because electric pumps would not work. Arizona, New Mexico, Oregon, Nevada, Texas, and Idaho experienced blackout-induced disruption in water service during the heat wave. In Fresno, where most of the city received water from wells powered by electric pumps, the city manager declared a local emergency. Only two of the city's 16 fire stations had water, and most of the fire hydrants were dry. Tankers were rushed in to supplement the fire department's water supply.
- ◆ Hurricane Andrew in August 1992 caused a blackout in South Florida that stopped water pumps from working. The blackout denied running water to hundreds of thousands of people stranded among the ruins left by Andrew, amidst Florida's summer heat. To meet the immediate crisis more than 200,000 gallons of water were distributed. However, without electricity to power radio or television sets, mass communication virtually ceased to exist, and people were unaware of relief efforts or where to seek help. Thousands may have been saved from dehydration by pyramids of bottled water on street corners made free for the taking and by survivors who spread the word.

In all the examples cited, timely emergency services to provide water prevented loss of life from dehydration. However, had the outages lasted longer and the blacked-out areas been larger, the outcome could have been very different. Storms are merely suggestive of, and provide some basis for extrapolating, the greater destructive effects on water infrastructure likely from an EMP attack.

Storm-induced blackouts and their effects on the water infrastructure are an imperfect analogy to EMP attack. Taken at face value, storm-induced blackouts and their consequences for the water infrastructure grossly understate the threat posed by an EMP attack. Storms are much more limited in geographic scope compared to an EMP attack. Power grid and water infrastructure recovery from storms, compared to recovery from an EMP attack, is likely to happen more quickly because of the "edge effect"—the capability of neighboring localities and states to provide recovery assistance. Because an EMP attack is likely to damage or disrupt electronics over a much wider geographic area than storm-induced blackouts, rescuers from neighboring states and localities would face a much bigger job, and recovery of the water infrastructure would take a much longer time.

Nor do storm-induced blackouts replicate the damage from an EMP attack that may occur in small-scale electronic systems critical to the operation of the water infrastructure, such as electric pumps, SCADAs, and motor controls for filters and valves. Compared to storms, an EMP attack is likely to inflict not only more widespread damage geo-



graphically, but also deeper damage, affecting a much broader array of electronic equipment, which will contribute to a more complicated and protracted period of recovery.

## Recommendations

A Presidential Directive establishes new national policy for protection of our nation's critical infrastructures against terrorist threats that could cause catastrophic health effects. National-level responsibilities have already been assigned to the Department of Homeland Security (DHS) and the Environmental Protection Agency (EPA) to protect the water infrastructure from terrorist threats. The EPA is the designated lead agency for protection of drinking water and water treatment systems. Under this directive:

- ◆ DHS and EPA should ensure that protection includes EMP attack among the recognized threats to the water infrastructure.
- ◆ The following initiatives should be amended:
  - The President's *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003), which details a plan for protecting the United States' critical infrastructures, including the infrastructure for water. The President's plan:
    - Identifies threats to the water infrastructure as: "Physical damage or destruction of critical assets...actual or threatened contamination of the water supply...cyber attack on information management systems...interruption of services from another infrastructure."
    - Directs the EPA to work with the DHS, state and local governments, and the water sector industry to: "Identify high-priority vulnerabilities and improve site security...improve sector monitoring and analytic capabilities...improve sector-wide information exchange and coordinate contingency planning...work with other sectors to manage unique risks resulting from interdependencies."
    - Focuses on terrorism and threats other than EMP, but lends itself well (in particular, its structure and logic) to addressing any threat, and should be amended to include EMP.
  - The *Public Health and Bioterrorism Preparedness and Response Act of 2002* (*Bioterrorism Act*), signed into law by President Bush on June 12, 2002. The Bioterrorism Act:
    - Requires the authorities over many drinking water systems to conduct vulnerability assessments, certify and submit copies of their assessments to the EPA, and prepare or revise their emergency response plans.
    - Is concerned with terrorist contamination of drinking water with chemical or biological agents.
    - Could be amended to address the greater bio-chemical threat that an EMP attack potentially poses to the water supply than any of the threats envisioned in the *Bioterrorism Act* because an EMP attack that causes SCADAs in water treatment facilities to malfunction could release biochemical agents, and conceivably contaminate water supplies over a very wide region.
- ◆ DHS and EPA should follow the government-recommended emergency preparedness steps applicable to a wide range of civil emergencies arising from different threats. These steps include assuring availability of water during emergencies. To that end, the government has recommended that citizens stockpile both water supplies and means of purification. Implementing these recommendations will provide some measure of preparation for an EMP threat to the water supply.

## Chapter 9. Emergency Services

### Introduction

Emergency services are essential to the preservation of law and order, maintenance of public health and safety, and protection of property. Americans have come to rely on prompt and effective delivery of fire, police, rescue, and emergency medical services through local government systems. Backing up these local systems are state capabilities (e.g., state police and National Guard) and specialized capabilities such as those provided by the Department of Homeland Security (DHS), the Department of Justice, the Centers for Disease Control and Prevention, and other federal entities.

*Americans have come to rely on prompt and effective delivery of fire, police, rescue, and emergency medical services.*

The demand for emergency services is large. Across the United States more than 200 million 9-1-1 calls are fielded annually.<sup>1</sup> Responding to these calls is an army of some 600,000 local law enforcement officers, 1 million firefighters, and more than 170,000 emergency medical technicians and paramedics.<sup>2</sup> Anticipated expenditures over the next 5 years for emergency response services are estimated at \$26 billion to \$76 billion at the state and local levels, supplemented by an additional \$27 billion at the federal level.<sup>3</sup>

Emergency services at all levels are receiving increased emphasis as a consequence of the September 11, 2001, terrorist attacks. The focus is on preventing and responding to terrorism, including nuclear attack, but little emergency services planning specifically considers electromagnetic pulse (EMP) attack.

*Little emergency services planning specifically considers EMP attack.*

The primary focus in this chapter is on local emergency services systems. In particular, this chapter focuses on the communications systems to alert, dispatch, and monitor those emergency services. The great majority of resources are concentrated at the local level; state and federal assistance will likely be quite thin, given the large geographic extent of an EMP attack.

In addition to local emergency systems, we also address the federal Emergency Alert System (EAS), designed to serve the President and other leaders in communicating with the public in emergency situations. Although no President has ever used the EAS, it is reasonable to anticipate that it would be used in the event of an EMP attack.

### Emergency Services Systems Architecture and Operations

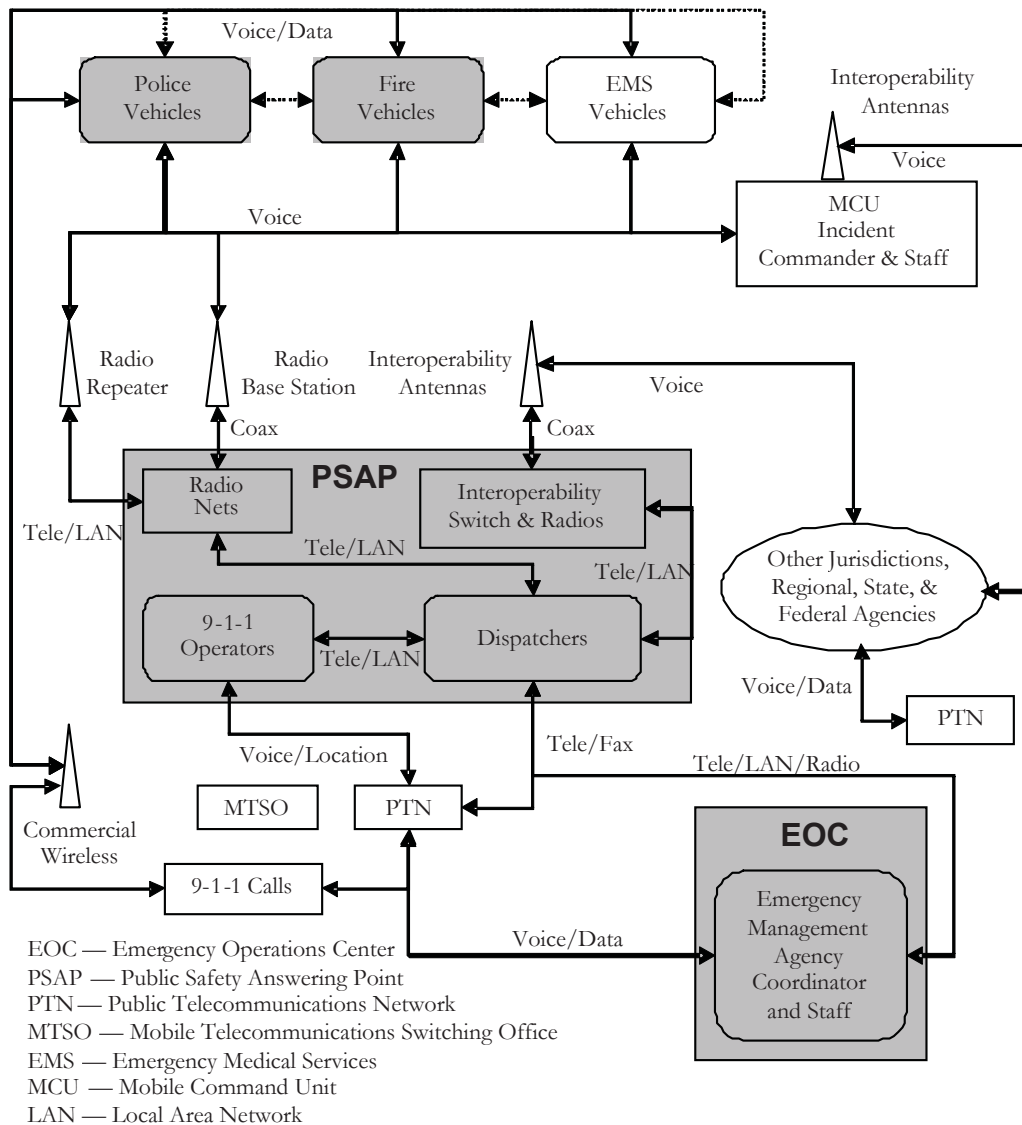
#### Local Emergency Services Systems

**Figure 9-1** depicts a generic modern local emergency service system. Shaded elements are those for which we have assessed EMP vulnerability, as discussed later in this chapter.

<sup>1</sup> National Emergency Number Association.

<sup>2</sup> Bureau of Labor Statistics. Frontline workers, including volunteers; excludes supervisory personnel.

<sup>3</sup> Rudman, Warren B., et al., *Emergency Responders: Drastically Underfunded, Dangerously Unprepared*, Council on Foreign Relations, 2003.



**Figure 9-1. A Generic Modern Emergency Services System**

Calls for assistance come in on cellular and land telephone lines to 9-1-1 operators at centers known as Public Safety Answering Points (PSAP). PSAPs typically include one or more 9-1-1 operators and dispatchers, communications equipment, computer terminals, and network servers. The 9-1-1 operator determines the service required and forwards the information for dispatch of the appropriate response units.

In addition to standard landline telephone service, emergency services employ a variety of wireless communication systems, including radio systems, cellular and satellite telephone systems, paging systems, messaging systems, and personal digital assistants. Because of dead zones and restrictions on radiated power levels in communications paths, radio repeaters are often used to relay voice and message traffic.

Because networks in nearby communities generally operate on different frequencies or channels to avoid interference, PSAP personnel use special equipment to handle community-to-community communications. If an emergency or public safety activity requires close and continuous coordination among several communities or agencies, an interop-

erability switch is used to allow direct communications among organizations. Interoperable communications across separate political jurisdictions is still a problem and under development in most regions.

For more serious emergencies, the Emergency Operations Center (EOC) serves as a central communications and coordination facility to which multiple organizations can send representatives. It facilitates efficient coordination across emergency services departments and state and federal agencies.

### **The Emergency Alert System**

The original motivation for the EAS (previously the Emergency Broadcast System and initially Control of Electromagnetic Radiation [CONELRAD]) was to provide the President the ability to communicate directly with the American people in time of crisis, especially enemy attack. Although it has never been used for that purpose, it has been activated in local emergencies and is widely used for weather alerts. The Federal Communications Commission (FCC) sets requirements through regulation of television and radio stations. The Federal Emergency Management Agency (FEMA), now part of DHS, provides administrative oversight.

In the case of a national emergency, a message is relayed from the President or his agent to high-power amplitude modulation (AM) radio stations, known as national primary stations, across the country. These stations broadcast signals to other AM and frequency modulation (FM) radio stations, weather radio channels, and television stations that, in turn, relay the message to still other stations, including cable television stations. These stations use encoders and decoders to send and receive data recognized as emergency messages.

### **Impact of an EMP Attack**

In a crisis, the priorities for emergency services are protection of lives, protection of property, effective communication with the public, maintenance of an operational EOC, effective communication among emergency workers, and rapid restoration of lost infrastructure capabilities. An EMP attack will adversely affect emergency services' ability to accomplish these objectives in two distinct ways: by increasing the demand for services and by decreasing the ability to deliver them.

### **Demand for Emergency Services**

The demand for emergency services will almost certainly increase dramatically in the aftermath of an EMP attack. These demands fall into two broad categories: *information* and *assistance*. The absence of timely information and the inability of recovery actions to meet the demand for emergency services will have grave consequences.

◆  
*The demand for emergency services will almost certainly increase dramatically in the aftermath of an EMP attack.*

Large-scale natural and technological disasters that have occurred in the last several decades demonstrate that information demands are among the first priorities of disaster victims. At the onset of a disaster, an individual is concerned primarily with his or her personal well-being and that of close family members and friends. The next most pressing concern is for information regarding the event itself. What happened? How extensive is the damage? Who was responsible? Is the attack over? A less immediate priority is for

information regarding recovery. How long will it take to restore essential services? What can and should I do for self-preservation and to contribute to recovery? It is important to recognize that emergency services providers also need all this information, for the same reasons as everyone else and also to manage recovery operations efficiently and perform their missions. Information assurance for emergency services requires reliable communications supporting the transport of emergency services such as enhanced 9-1-1 (E9-1-1).<sup>4</sup> As discussed in Chapter 3, Telecommunications:

Based upon results of the Commission-sponsored analysis, an EMP attack would disrupt or damage a functionally significant fraction of the electronic circuits in the Nation's civilian telecommunications systems in the region exposed to EMP. The remaining operational networks would be subjected to high levels of call attempts for some period of time after the attack, leading to degraded telecommunications services.

To meet the demand for priority national security and emergency preparedness (NS/EP) services supporting first responders, the FCC and the DHS's National Communications System (NCS) offer a wide range of NS/EP communications services that support qualifying federal, state, and local government, industry, and nonprofit organization personnel in performing their NS/EP missions, including E9-1-1 PSAPs.<sup>5,6</sup>

The demand for assistance will increase greatly in the event of an EMP attack. The possibility of fires caused by electrical arcing resulting from an EMP attack cannot be ruled out. There is no reliable methodology to predict the frequency of such fires. As with other EMP effects, however, they will occur near-simultaneously, so that even a small number could overwhelm local fire departments' ability to respond. Fires indirectly caused by an EMP attack, principally because of people being careless with candles used for emergency lighting or with alternative heating sources during power blackouts, are also a concern.

There also exists the possibility of EMP-caused airplane crashes.<sup>7</sup> The average daily peak of air traffic in U.S. airspace includes more than 6,000 commercial aircraft carrying some 300,000 passengers and crew. Commercial aircraft are protected against lightning strikes but not specifically against EMP. The frequency composition of lightning and EMP differ enough so that lightning protection does not ensure EMP protection. On the other hand, the margins of safety for lightning protection imposed on commercial aircraft may provide flight safety in the event of an EMP attack. In any event, we cannot rule out the possibility of airplane crashes.

Debilitating EMP effects on the air traffic control system will also be a contributing factor to airplane crashes.

Emergency rescue services can be expected to experience an increase in demand. People trapped on subways and in elevators will require timely rescue. If electric power is interrupted for any period of time, people at home who depend on oxygen concentrators, respirators, aspirators, and other life-sustaining equipment that require electric power will need to find alternative solutions quickly. Home backup systems, including oxygen tanks, liquid oxygen supplies, and battery and generator power, will lessen the need for an

<sup>4</sup> E9-1-1 provides emergency services personnel with geographic location information on mobile callers.

<sup>5</sup> PSAP Enrollment in the TSP Program, <http://www.nasna911.org/pdf/tsp-enroll-guide.pdf>.

<sup>6</sup> National Communication System, <http://www.ncs.gov/services.html>.

<sup>7</sup> See also Chapter 6, Transportation Infrastructure.



immediate response for those fortunate enough to have them, but eventually all these people will need to be transported to facilities with a reliable power source and appropriate equipment. If power is out for more than several days, people dependent on dialysis machines, nebulizers, and other life-supporting medical devices also will be at risk. Finally, inability to replenish home supplies of medicines will eventually lead still more people to depend on emergency services.

Police services will be stretched extremely thin because of a combination of factors. Police will be called on to assist rescue workers in removing people from immediate dangers. Failures of automobiles and traffic control systems with attendant massive traffic jams will generate demands for police services for traffic management. Antisocial behavior also can occur following a chaotic event. Though it is more commonly seen in disasters originating from conflict, such as riots, than from natural or technological disasters, opportunistic crime (because of failures of electronic security devices, for example) is a potential reaction to an EMP attack. While not as prevalent as may be perceived, far worse antisocial behavior such as looting also could occur, especially in communities that experience conflict because of shortages or in areas that experience high crime rates under nondisaster circumstances. If looting or other forms of civil disorder break out, it is likely that local police services will be overwhelmed. In that event, deployment of National Guard forces, imposition of curfews, and other more drastic measures may be necessary.

Although emergency services could be completely overwhelmed in the aftermath of an EMP attack, it is important to recognize that the demand for emergency services could be ameliorated somewhat

◆  
*Emergency services could be completely overwhelmed in the aftermath of an EMP attack.*

by citizen groups that frequently emerge in the aftermath of disasters to lead or assist in recovery efforts. In the absence or failure of government-provided emergency services, these groups may take on roles similar to those services, for example, by moving and providing basic household necessities to families in need, clearing debris, or serving as an impromptu communications network. This example of prosocial behavior is not uncommon in the aftermath of natural disasters such as hurricanes, floods, or earthquakes. This was seen following the September 11, 2001, terrorist attacks, when thousands of New York citizens volunteered to give blood, help firefighters and police at the World Trade Center grounds, and assist in other ways.

On the other hand, when the failure of police and emergency services becomes protracted, the lawless element of society may emerge. For example, Hurricane Katrina in August 2005 damaged cell phone towers and radio antennas that were crucial to the operation of emergency communications. Protracted blackout of the power grid caused generators supporting emergency communications to exhaust their fuel supplies or fail from overuse. Consequently, government, police, and emergency services were severely impacted in their ability to communicate with the public and with each other. Looting, violence, and other criminal activities were serious problems in the aftermath of Katrina. In one instance, the Danziger Bridge incident<sup>8</sup>, members of a repair crew came under fire. Police called to the scene returned fire, and a number of people were killed. An EMP

---

<sup>8</sup> Burnett, John. "What Happened on New Orleans's Danziger Bridge?" <http://www.npr.org/templates/story/story.php?storyId=6063982>.

attack is likely to incapacitate the same nodes—cell phone towers and radio antennas—and overtax generators supporting emergency communications for a protracted period, creating the same conditions that incited lawless behavior in the aftermath of Katrina.

### **EMP Effects on Emergency Services**

Some equipment needed to perform emergency services will be temporarily upset or directly damaged by an EMP attack, resulting in diminished capabilities during the time of greatest demand.

*An EMP attack will result in diminished capabilities during the time of greatest demand.*

Little, if any, emergency services equipment has been hardened specifically against EMP and thus may be vulnerable. On one hand, both communications equipment and vehicles commonly employed in the emergency services infrastructure generally have been designed to cope with the increasingly dense everyday electromagnetic environment from radio, television, wireless communications, radar, and other man-made sources. On the other hand, emergency services rely on radios to transmit and receive voice and message traffic using many frequencies, including the same frequencies contained in EMP radiation fields. Whether or not this results in degradation depends on the effectiveness of any built-in protection devices in these radios as well as the internal robustness of the radio itself.

To gauge the degree of vulnerability of emergency services to EMP, the Commission conducted an assessment of emergency services equipment and associated networks.<sup>9</sup> We tested a representative variety of key electronics-based equipment needed by national leadership, first responders, and the general population. In most cases, only one of each model was tested, so statistical inferences are not possible from our test data. Moreover, a more robust assessment would test equipment under a range of conditions (such as different orientations, equipment operating modes, and test waveforms). Thus, our assessment should be viewed as indicative, rather than definitive. Notwithstanding these caveats, these tests are the most comprehensive recent vulnerability tests of emergency services equipment to date.

Our testing concentrated on items that were found to be critical for local emergency services and the EAS. The testing used standard EMP test practices, including radiated pulse and direct current injection test methods. Large-scale and smaller radiated pulse simulators were used to illuminate the equipment with an approximation of the electromagnetic field generated by an actual EMP event. A second test method, known as pulse current injection, accounted for the stresses coupled to long lines such as power feeds that cannot be accurately tested in a radiated simulator. We also used the results of relevant past EMP testing efforts.

**Public Safety Answering Points.** The key elements of a PSAP include commercial telephone links for incoming 9-1-1 calls, computer-aided dispatch, public safety radio, and mobile data communications. There are other elements associated with PSAPs, but this is the minimal set necessary to provide emergency response to the public.

Computers are essential to normal PSAP operations. Recent personal computer equipment tests covered a wide technology range, consistent with what is typically in use in

<sup>9</sup> Radasky, William A., *The Threat of Intentional Electromagnetic Interference (IEMI) to Wired and Wireless Systems*. Metatech Corporation, Goleta, California, 162.

PSAPs. Results indicate that some computer failures can be expected at relatively low EMP field levels of 3 to 6 kilovolts per meter (kV/m). At higher field levels, additional failures are likely in computers, routers, network switches, and keyboards embedded in the computer-aided dispatch, public safety radio, and mobile data communications equipment.

A variety of mobile radios were tested in the stored, dormant, and operating states, in both handheld and vehicle-mounted configurations. Consistent with older test data,<sup>10</sup> none of the radios showed any damage with EMP fields up to 50 kV/m. While many of the operating radios experienced latching upsets at 50 kV/m field levels, these were correctable by turning power off and then on. However, most of the fixed installation public safety radio systems include telecommunication links between the computer-aided dispatch terminals and the main or repeater radio units. Therefore, because of computer failures in dispatch equipment, communication system failures might occur at EMP field levels as low as 3 to 6 kV/m.

Based on these results, we anticipate that several major functions of PSAPs will be affected by an EMP attack. The significance and duration of the impact of these failures will depend on multiple factors such as the ability of technical staff to repair or replace damaged equipment and the existence of plans and procedures to cope with the specific type of failure. For example, based on a review of representative Y2K public safety contingency plans, loss of the computer-aided dispatch capability can be overcome by the use of simple note cards for manually recording the information needed for dispatch. However, loss of the mobile radio communications or the incoming commercial telecommunications functions could be more difficult to counteract. Typically, local jurisdictions rely on nearby PSAPs or alternate locations to overcome these types of failures. In an EMP attack, these contingency plans may fail because of the wide area of effects.

*Interoperability Switches.* These switches are contained in many PSAPs to facilitate direct communications among local, regional, and state public safety departments and federal agencies after major disasters. The main elements of the interoperability switch capability are the public safety radios, the switch unit itself, and the computer network link between the switch unit and the dispatch console. The public safety radios that were tested as part of this assessment were based on the equipment used in a fully operational interoperability switch.<sup>11</sup> The testing was performed with the equipment in stored, dormant, and operating states. No failures were experienced at test levels up to 50 kV/m. The interoperability switch was also tested up to 50 kV/m with no adverse effects.

Based on these results, the interoperability switch capability is expected to function normally after an EMP attack. However, the computer network link between the interoperability switch and the dispatch station may fail at field levels as low as 3 to 6 kV/m. This would necessitate manual operation of the switch to implement the connections among various law enforcement, fire, and EMS agencies.

*Vehicles.* Emergency service vehicles include police cars, fire trucks, and EMS vehicles. An extensive test of a police car was performed. The most severe effect found

<sup>10</sup> Barnes, Paul R., *The Effects of Electromagnetic Pulse (EMP) on State and Local Radio Communications*, Oak Ridge National Laboratory, October 1973.

<sup>11</sup> Metropolitan Interoperability Radio System — Alexandria Site Description Document, *Advanced Generation of Interoperability for Law Enforcement (AGILE)*, Report No. TE-02-03, April 4, 2003.

was the latch-up of a mobile data computer at approximately 70 kV/m. After rebooting, the computer functioned normally.

Electronic equipment found on many of the mobile units also was tested. This equipment included a computer, personal data assistant, mobile and portable radios, defibrillators, and vital signs monitors. No permanent failures were experienced at levels up to 70 kV/m. Thus, we anticipate that the electronics in emergency services mobile units will continue to function normally, but they may suffer some initial effects due to latching upset of electronic devices.

*Emergency Operation Centers.* A site survey was performed at the Virginia state EOC. The survey confirmed that the vast majority of EOC communications depends on the Public Telecommunications Network (PTN). Thus, the ability of the EOC personnel to communicate and therefore provide emergency coordination will be highly dependent on the capability of the public telecommunications infrastructure to operate after an EMP event.

EOCs typically have at least one FEMA-owned and -maintained high-frequency (HF) radio for connectivity among national, regional, and state EOCs. The survivability of these HF radio units was not assessed. However, the operating band of these radios is one factor that makes them potentially vulnerable to EMP attack. Backup communications links may include satellite telephone systems and capabilities provided by amateur radio operator organizations.

EOCs also contain electronic equipment such as personal computers and digital data recorders. As with PSAPs, the capabilities supported by such equipment are vulnerable to EMP field levels as low as 3 to 6 kV/m.

Some EOCs are located below ground, which provides some protection from radiated EMP fields. However, conductive lines penetrating into these facilities must still be protected to ensure EMP survivability.

*The Emergency Alert System.* The primary method of initiating an emergency alert message involves the use of multiple commercial telecommunications lines. Therefore, the ability to provide emergency alert messages depends first on the status of the commercial telecommunications system. Broadcast of an alert message and receipt by the affected public depends on several electronic systems, including commercial radio and television stations, EAS multimodule receivers and encoders/decoders, and commercial radio and television receivers.

We performed site surveys of both a radio station and a television station. Backup power generators and spare transmitter equipment were found at both facilities. While not all commercial broadcast stations include such backup systems, the EAS has significant redundancy; some, but not all, broadcast stations are necessary for successful transmission of an emergency alert message.

We tested commonly used multimodule receiver and encoder/decoder units. The AM receiver module in its dormant mode failed at a field level of 44 kV/m. The FM receiver module exhibited erratic signal levels at 50 kV/m. No other effects were noted in testing EAS-specific equipment.

Four different television sets and two different radio receivers were tested. The vehicle testing performed for the transportation infrastructure assessment also tested radios in

vehicles. In one AM radio installed in a vehicle, a malfunction occurred at approximately 40 kV/m. All other items showed no malfunctions.

Based on these results, we expect that the EAS will be able to function in near-normal fashion following an EMP attack. The major impact that might occur is a delay in initiation and receipt of an alert message because of (1) the dependency on the commercial telecommunications system, (2) the loss of some receiver channels for the EAS equipment, (3) the potential loss of some radio and television stations from power loss or damage to transmitter components, and (4) the loss of some AM radio receivers.

**Interdependencies.** In addition to direct damage, emergency services will be degraded to the extent that they are dependent on other infrastructures that are themselves damaged by the EMP attack. Emergency services are most directly dependent on the electric power, telecommunications, transportation, and fuel infrastructures. Fire departments also are dependent on the availability of water. EMP damage to these infrastructures can seriously degrade emergency services.

Of particular importance, emergency services are heavily dependent on the ability of the Nation's PTN to process 9-1-1 calls in a timely manner. After an EMP event, the PTN is likely to experience severe delays in processing calls.<sup>12</sup> Since 9-1-1 calls are processed using the same PTN equipment as non-9-1-1 calls (until they reach special 9-1-1 call-processing equipment located in a tandem central office assigned to each PSAP), they will be subject to delays similar to those for nonemergency calls. In the short term, this will result in a large number of lost 9-1-1 calls. After several days, the operation of the PTN is expected to return to near normal, assuming no adverse effects from either extended widespread power outages or from an inability to replenish fuel supplies for backup generators. However, in the event of a widespread power outage that extends beyond the time that backup power is available or commercial power service is restored, the PTN's ability to process 9-1-1 calls will again degrade. Eventually, extended widespread power outages will result in an inability to replenish fuel supplies, essentially causing a complete loss in PTN capability to process any 9-1-1 calls.

Loss of power can also directly impact PSAP operations. In the short term, the loss of commercial power will impact local emergency services more from the standpoint of increased calls for assistance than from functional impact. Most PSAPs and EOCs have backup power generators that will allow uninterrupted operation for some time period. Long-term power outages might result in the loss of PSAPs and EOCs because of an inability to refuel the backup generators.

### Consequences

The ultimate consequences of an increased demand for emergency services and a concomitant degradation in emergency services capabilities are measured in lives lost, health impaired, and property damaged. We have no way of accurately estimating these consequences; we can only cite suggestive statistics.

*We have no accurate way to measure the impact of degraded emergency services on lives lost, health impaired, or property damaged.*

<sup>12</sup> See Chapter 3, Telecommunications.



Most importantly, we note that the lives and health of many people depend on medical technologies that, in turn, depend on electric power. People will turn to emergency services if that power is unavailable for an extended period.

Emergency medical services respond to approximately 3 million 9-1-1 calls annually for people with cardiac problems and 2.5 million others for respiratory problems.<sup>13</sup>

Fire departments responded to 1,687,500 fires in 2002. These fires resulted in property damage estimated at \$10.3 billion and 3,380 civilian deaths.<sup>14</sup> Lives and property saved by fire departments are undoubtedly also very large numbers.

Other direct consequences would result from the inability to successfully place a 9-1-1 call. Missed 9-1-1 calls can result from any number of causes, including (1) PTN outages; (2) EMP-induced damage to PSAPs, PSAP repeaters, mobile communications, or other critical support equipment; and (3) failure of commercial or residential telephone equipment.

The principal indirect consequences of a decline or collapse of emergency services are a result of a reduction in the availability of the work force. We did not attempt to quantify this effect, but note that it includes not only those directly affected, but also those who must now support those who previously would have depended on emergency services.

## Recommendations

Our recommended strategy for protection and recovery of emergency services emphasizes the establishment of technical standards for EMP protection of critical equipment and the inclusion of EMP in planning and training.

The technology for critical emergency services functions is undergoing extensive change, creating an excellent opportunity for inclusion of our recommended protection measures. This technology change is propelled in large part by the need for additional emergency services communications capability and the recognition that large-scale disasters, such as the terrorist attacks of September 11, 2001, require extensive coordination across the full spectrum of emergency services providers.

Our strategy can be realized through implementation of the following recommendations:

- ◆ DHS and state and local governments should augment existing plans and procedures to address both immediate and long-term emergency services response to EMP attack. Plans should include provisions for a protection and recovery protocol based on graceful degradation and rapid recovery that emphasizes a balance between limited hardening and provisioning of spare components. Such a plan should ensure the following:
  - The National Emergency Number Association should establish guidelines for operability and recovery of PSAPs during and after exposure to EMP.
  - The FCC should task the Network Reliability and Interoperability Council to address the NS/EP services,

◆ *Our recommended strategy for protection and recovery of emergency services emphasizes the establishment of technical standards for EMP protection of critical equipment and the inclusion of EMP in planning and training.*

<sup>13</sup> Estimates based on a survey of local PSAPs, extrapolated to the entire country.

<sup>14</sup> Statistics obtained from the National Fire Protection Association.

such as E9-1-1, and identify best practices to prevent, mitigate, and recover from an exposure to EMP.

- ◆ DHS should provide technical support, guidance, and assistance to state and local governments and federal departments and agencies to ensure the EMP survivability of critical emergency services networks and equipment. To accomplish this, the DHS should take the following actions:
  - In coordination with the Department of Energy and other relevant government entities, develop a set of EMP recovery scenarios that include coordinated attacks involving EMP and other more widely understood threats involving weapons of mass destruction.
  - In coordination with relevant government agencies, work with the appropriate standards entities (e.g., the Association of Public-Safety Communications Officials, the National Emergency Number Association, and the International Electrotechnical Commission) to establish EMP immunity standards and guidelines for critical emergency services equipment.
  - Develop training courses for emergency services providers on how to enhance immunity to, operate during, and recover from an EMP attack.
  - Develop an EMP attack consequence assessment tool to perform planning analysis and training and to assist in the identification of critical equipment and manpower requirements.
  - Establish a program to assess the vulnerability of evolving emergency services networks and electronics equipment to EMP and to develop a model plan for hardness maintenance and surveillance for implementation by state and local jurisdictions.



## Chapter 10. Space Systems

### Introduction

Over the past few years, there has been increased focus on U.S. space systems in low Earth orbits and their unique vulnerabilities, among which is their susceptibility to nuclear detonations at high altitudes—the same events that produce EMP. It is also important to include, for the protection of a satellite-based system in any orbit, its control system and ground infrastructure, including up-link and down-link facilities.

Commercial satellites support many significant services for the Federal Government, including communications, remote sensing, weather forecasting, and imaging. The national security and homeland security communities use commercial satellites for critical activities, including direct and backup communications, emergency response services, and continuity of operations during emergencies. Satellite services are important for national security and emergency preparedness telecommunications because of their ubiquity and separation from other communications infrastructures.

The Commission to Assess United States National Security Space Management and Organization conducted an assessment of space activities that support U.S. national security interests and concluded that space systems are vulnerable to a range of attacks due to their political and economic value.<sup>1</sup> Satellites in low Earth orbit generally are at risk of lifetime degradation or failure from collateral radiation effects arising from an EMP attack on ground targets.

In the course of an EMP attack, a nuclear detonation at a high altitude produces numerous other effects that can impact the performance and survival of satellites. Examination of these effects relates to the Commission's mandate in two ways. First, nuclear weapon effects on satellites can be collateral consequences of an EMP attack. Second, an EMP attack can degrade ground terminals that satellite systems require for uplinks, downlinks, and control functions.

This chapter focuses on two classes of effects that are primary threats to the physical integrity of satellites: (1) direct, line-of-sight exposure to nuclear radiation pulses (e.g., X-ray, ultraviolet, gamma-ray, and neutron pulses) and (2) chronic exposure to enhanced high-energy electrons durably trapped in the Earth's magnetic field. These effects can jeopardize satellites in orbit, as data from U.S. and Soviet high-altitude nuclear tests of 1958 and 1962 attest. **Figure 10-1** illustrates visible phenomena from several U.S. high-altitude nuclear tests. Each detonation produced copious X-ray fluxes and trapped energetic electron radiation in space. When the United States detonated the 1.4-megaton (MT) STARFISH<sup>2</sup> device on July 9, 1962, at 400 km altitude, a total of 21 satellites were in orbit or were launched in weeks following. Eight suffered radiation damage that compromised or terminated their missions.<sup>3</sup> Information concerning the fate of the remaining 13 satellites is not publicly available.

---

<sup>1</sup> Report of the Commission to Assess United States National Security Space Management and Organization, January 11, 2001.

<sup>2</sup> The high-altitude test originally known as STARFISH was not successful. A second high-altitude test called STARFISH PRIME was successfully executed at a later date to obtain the sought-after data. In much of the literature describing the damage to satellites from this test, the name of the event is called STARFISH without the PRIME modifier. For the sake of brevity we also have dropped the modifier.

<sup>3</sup> Brown, W.L., W.N. Hess, and J.A. Van Allen, "Collected Papers on the Artificial Radiation Belt From the July 9, 1962, Nuclear Detonation," *Journal of Geophysical Research* 68, 605, 1963.

In many respects, satellite electronics of the 1960s were relatively robust against nuclear effects. Their bulk and comparatively low-speed operation tended to make electronics of the era substantially less vulnerable to radiation upset and damage than modern electronics at comparable exposure levels. The discussion to follow highlights salient points of satellite vulnerabilities to nuclear explosions in the upper atmosphere or space. These vulnerabilities are considerable and incontrovertible — each worldwide fleet of satellites is at risk, but the degree of risk depends on the extent of satellite hardening, satellite location relative to the burst, resultant line-of-sight exposure to prompt radiations, and each satellite's exposure to geomagnetically trapped energetic particles of natural and nuclear origins.

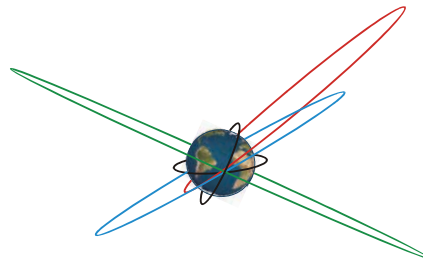


**Figure 10-1.** From left to right, the ORANGE, TEAK, KINGFISH, CHECKMATE, and STARFISH high-altitude nuclear tests conducted in 1958 and 1962 by the United States near Johnston Island in the mid-Pacific. Burst conditions for each were unique, and each produced strikingly different phenomena and different enhancements of the radiation belts.

### Terms of Reference for Satellites

Ubiquitous Earth-orbiting satellites are a mainstay of modern critical national infrastructures. Satellites provide Earth observations, communications, navigation, weather information, and other capabilities. The United States experienced significant disruption when the pager functions of PanAmSat Galaxy IV failed in May 1998.

Each satellite's orbit is optimized for its intended mission. Low Earth orbits (LEO), from 200 to 2,000 km altitude, are in proximity to the Earth and atmosphere to enable remote sensing, weather data collection, telephony, and other functions. Geosynchronous (a.k.a. geostationary) orbits (GEO) lie at about 36,000 km altitude in the equatorial plane, where their 24-hour orbital period matches the rotation of the Earth. This orbit allows GEO satellites to hover above a fixed longitude, useful for communications and monitoring of large-scale weather patterns. Satellites in highly elliptical orbits (HEO) perform specialized functions inaccessible to other orbits. For example, HEO satellites in high inclination orbits provide wide-area communications above high-latitude regions for several hours at a time. **Figure 10-2** illustrates common orbits.



**Figure 10-2. Satellite Orbits Illustrated.** Geosynchronous orbit (green) in the equatorial plane is at about 36,000 km altitude. LEO (black) are shown with inclinations relative to the equatorial plane of 30° and 90°, but any inclination is possible. A 45° inclination orbit at approximately 20,000 km altitude is shown in blue. HEO are shown in red.

### Line-of-Sight Exposure to a Nuclear Detonation

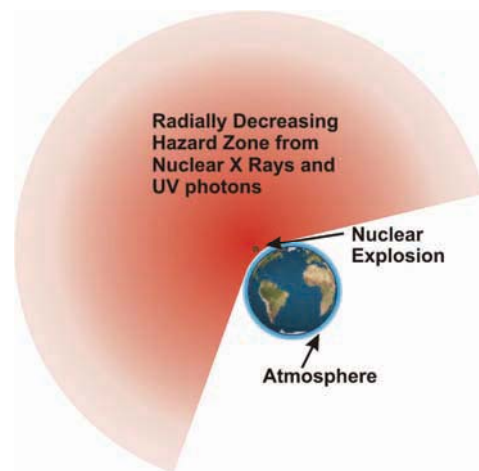
A nuclear device will, upon detonation, radiate a portion of its total yield as X-rays, with the fraction realized a function of weapon design and attached delivery system.



Attenuation of X-rays propagating through the upper atmosphere is primarily by photoelectric absorption by oxygen and nitrogen and therefore is a function of X-ray spectrum, with higher-energy photons penetrating greater path-integrated mass density along the line of sight. Consequently, for a detonation above a (spectrally dependent) threshold altitude, X-rays emitted horizontally or upward will propagate to large distances virtually unattenuated by the atmosphere. X-rays emitted downward will be absorbed over ranges of tens of kilometers upon reaching sufficiently dense air.

Neutrons and gamma rays emitted by a detonation similarly propagate upward great distances into space for detonations above threshold altitudes. However, owing to scattering and absorption cross sections substantially smaller than X-ray photoelectric cross sections, major atmospheric attenuation of these energetic emissions occurs at altitudes below approximately 40 km.

For detonations up to a few hundred kilometers altitude, blast wave interactions between expanding weapon debris and the atmosphere may convert a majority of the kinetic yield of the weapon to ultraviolet (UV) photons. These photons propagate upward into space with little attenuation. UV photons emitted horizontally and downward are absorbed in the vicinity of the burst point to form the UV fireball. UV production for bursts above a few hundred kilometers declines rapidly, with precise values for these transition altitudes being functions of weapon output characteristics and dynamics. The combined flux of energetic photons (X-ray, gamma, and UV) and neutrons irradiates a vast region of space, diminished by spherical divergence, as shown in **figure 10-3**. The actual size of the hazard zone depends on weapon yield, detonation altitude, and the degree of satellite hardening against disruption or harm. Damage to satellite structures and to coatings on solar panels and sensor optics occurs when X-ray and UV fluxes exceed critical thresholds. Electronics damage similarly ensues when X-ray and gamma pulses induce destructive electric currents in circuit elements and when energetic neutrons penetrate solid-state circuitry.



**Figure 10-3. Areas of Space Irradiated by Photons and Neutrons.** Where not shadowed by the Earth or shielded by atmospheric attenuation, X-rays and UV photons travel great distances from a high-altitude nuclear detonation where they may inflict damage to satellites.

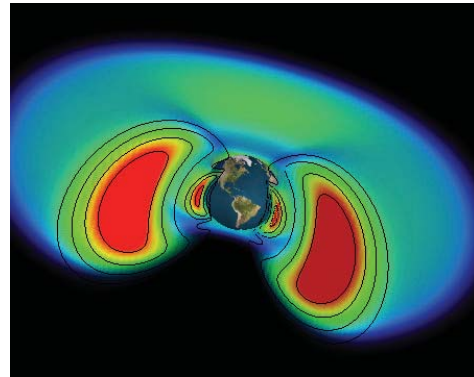
## Persistently Trapped Radiation and Its Effects

In 1957, N. Christofilos at the University of California Lawrence Radiation Laboratory postulated that the Earth's magnetic field could act as a container to trap energetic electrons liberated by a high-altitude nuclear explosion to form a radiation belt that would encircle the Earth.<sup>4</sup> In 1958, J. Van Allen and colleagues at the State University of Iowa used data from the Explorer I and III satellites to discover the Earth's natural radiation belts.<sup>5</sup> **Figure 10-4** provides an idealized view of the Van Allen belts. Later in 1958, the United States conducted three low-yield ARGUS high-altitude nuclear tests, producing nuclear radiation belts detected by the Explorer IV satellite and other probes. In 1962, larger tests by the United States and the Soviet Union produced more pronounced and longer lasting radiation belts that caused deleterious effects to satellites then in orbit or launched soon thereafter.

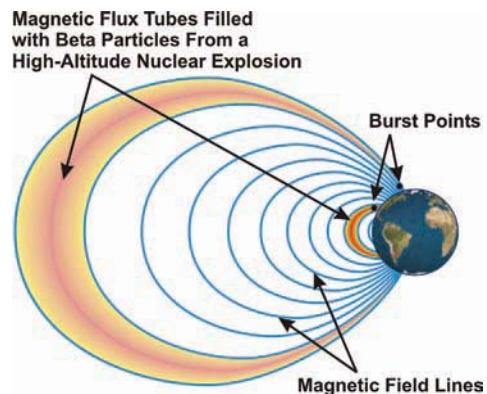
A nuclear detonation is a significant source of free electrons originating from the highly ionized plasma that is a product of the nuclear blast. Nuclear detonations also create trapped radiation by beta decay of radioactive weapon debris and free-space decay of neutrons from the explosion, thereby creating electrons with energies up to several million electron volts (MeV). The most notable tests producing radiation hazards to satellites were the U.S. STARFISH detonation and three high-altitude tests by the Soviets, all conducted in 1962.

One assesses natural and trapped nuclear radiation effects on contemporary satellites by calculating repeated passage of a satellite through radiation belts over the satellite's lifetime. While the geometry of a satellite's orbit is relatively straightforward, characterization of spatial and temporal properties of both natural and nuclear radiation belts is a complex problem. Nevertheless, one can establish relative scaling of levels of vulnerability from radiation belt geometry, as shown in **figure 10-5**. Intensities of radiation belts depend strongly on burst latitude. A burst at low latitude fills a small magnetic flux tube volume, so trapped flux tends to be concentrated and intense. The same burst at higher latitude fills a much larger magnetic flux tube volume.

All quantitative assessments of effects on satellite lifetime provided in this chapter are based on calculations carried out using a code that tracks the satellite orbits through space and calculates the accumulated radiation dose.



**Figure 10-4.** Naturally occurring belts (Van Allen belts) of energetic particles persistently trapped in the geomagnetic field are illustrated.



**Figure 10-5.** Schematic diagram of relative intensities of trapped fluxes from two identical high-altitude nuclear detonations.

<sup>4</sup> Christofilos, N.C., Proceedings of the National Academy of Sciences, U.S. 45, 000, 1959.

<sup>5</sup> Van Allen, J.A., and L.A. Frank, "Radiation Around the Earth to a Radial Distance of 107,400 km," *Nature*, 183, 430, 1959.

## **Nuclear Weapon Effects on Electronic Systems**

Electronic systems perform many critical spacecraft functions. An electronic power control system regulates the energy obtained from the solar cells. Attitude control circuits keep the vehicle oriented so that solar panels receive maximum exposure to the sun and sensors face the Earth. Information collected by sensors must be processed, stored, and transmitted to the Earth on demand. Communications satellites receive information, possibly process it, and then retransmit it, all by electronic circuits. Both prompt and long-term radiation effects have the potential for corrupting these functions in systems that lack hardening or other mitigation of nuclear effects.

### ***Total-Dose Damage***

A common criterion for failure of an electronic part is the total radiation energy per unit volume deposited in silicon. This absorbed energy density is expressed in rads(Si) (1 rad = 100 ergs/gram). Natural radiation to an electronic part in the International Space Station (ISS) behind a 2.54 mm semi-infinite (very large) aluminum slab averages about 100 rads per year. Previous literature has commonly used this shielding thickness for satellite radiation exposure calculations. However, it should be noted that electronics are placed in a variety of locations in a satellite and, therefore, can have different levels of shielding. Natural radiation to an electronic part in LEO, such as the National Oceanic and Atmospheric Administration (NOAA) satellite, in polar orbit behind a 2.54 mm semi-infinite aluminum slab is, on long-term average, about 620 rads per year, while some satellites with the same shielding might receive 50 kilorads per year.<sup>6</sup> Electronics must be shielded in accordance with the intended orbit to limit the dose received to a tolerable level.

### ***Radiation-Induced Electrostatic Discharge***

One hazard to spacecraft passing through the natural or nuclear radiation belts is internal or “deep dielectric” charging.<sup>7</sup> Lower-energy electrons (40 to 300 keV) become embedded in surface materials or poorly shielded internal materials and, on a timescale of hours to days, can build up sufficient electric field to cause a discharge, often resulting in satellite upset and occasionally in serious damage. Thermal blankets, external cables, and poorly shielded circuit boards are prime candidates for this type of charging. Modern coverglasses and optical solar reflectors are made sufficiently conductive to avoid such local charge buildup.

### ***Radiation Effects Assessment and Hardening***

Susceptibility of electronic components to nuclear weapon radiation has been studied intensively both experimentally and analytically since 1956. State-of-the-art computers and algorithms are used to extrapolate the experimental results to an operational environment.

The EMP Commission’s mission was to evaluate the threat of high altitude nuclear weapon-induced EMP on American national infrastructure. A collateral result of a high altitude burst is a radiation threat to satellites, primarily those residing in LEO. The damage manifests as upset or burnout of sensitive microelectronics on the spacecraft. In some

---

<sup>6</sup> Schreiber, H., “Space Environments Analyst, Version 1.2,” 1998 Space Electronics, Inc., Calculations using Space Radiation 4.0, Space Radiation Associates, Eugene, OR, 1998.

<sup>7</sup> Frederickson, A.R., “Radiation-Induced Dielectric Charging in Space Systems and Their Interactions with Earth’s Space Environment,” eds. H.B. Garrett and C.P. Pike, Progress in Astronautics and Aeronautics, vol. 71, AIAA, 1980.

cases, damage can occur to external surfaces and structural members, as well as to optical components and to solar-cell power sources.

To address these issues, we considered a plausible set of 21 EMP nuclear events, which are listed in **table 10-1**. These disparate threats were then imposed upon a set of satellites (**table 10-2**) representative of the U.S. space infrastructure to examine the ancillary effects of an exoatmospheric nuclear detonation.

The time frame of interest is through the year 2015. As indicated in **table 10-1**, cases include both higher and lower yield weapons. Though not included in **tables 10-1** through **10-6**, each event is also associated with a particular latitude and longitude.

**Table 10-1. Trial Nuclear Events**

Event	Yield (kT)	Height of Burst (km)	L-Value <sup>8</sup>
1	20	200	1.26
2	100	175	1.09
3	300	155	1.09
4	10	300	1.19
5	100	170	1.16
6	800	368	1.27
7	800	491	1.36
8	4,500	102	1.11
9	4,500	248	1.16
10	30	500	1.23
11	100	200	1.18
12	20	150	1.24
13	100	120	1.26
14	500	120	1.26
15	100	200	1.03
16	500	200	1.03
17	5,000	200	1.03
18	1,000	300	4.11
19	10,000	90	4.19
20	1,000	350	6.85
21	10,000	90	6.47

While the primary threat from nuclear-pumped radiation belts is to satellites in relatively low orbits, high-yield bursts could be detonated at latitudes and longitudes that would threaten higher orbiting satellites (Events 18 to 21). These bursts would be at relatively high latitudes sufficient to allow high-energy electrons to migrate along geomagnetic field lines that reach the high altitudes at which geosynchronous satellites reside.<sup>9</sup> Of course, at higher orbital altitudes, the density of ionizing radiation would be much reduced over that experienced by a satellite orbiting at lower altitudes and

<sup>8</sup> It is conventional (and useful) to describe the magnetic field lines on which electrons are trapped as belonging to numbered L-shells. The L-value of a field line is the distance (in Earth radii measured from the location of Earth's dipole field source) at which the field line intersects the magnetic equator. The inner belt peaks around L = 1.3, and the outer belt, near L = 4. Trapped electrons rapidly gyrate about the field lines, bounce along the field lines between mirror points, and drift around the Earth.

<sup>9</sup> As illustrated in **figure 10-5**, magnetic field lines that intersect the Earth at high northern and southern latitudes extend outward into space to relatively large distances. Conversely, magnetic field lines that intersect the Earth at low latitudes extend relatively short distances into space. Consequently, geomagnetically trapped electrons created by detonations at high latitudes can propagate along field lines out to very high altitudes where satellites orbit, whereas trapped electrons created by low-latitude bursts would be less likely to do so.

subjected to the same nuclear source due to the much larger volume in which the ionizing energy is distributed.

**Table 10-2. Analysis of Satellites**

Satellite	Altitude (km)	Mission
NOAA/DMSF	800 (LEO)	Weather, remote sensing, search and rescue
TERRA/IKONOS	700 (LEO)	Moderate-high resolution imaging Earth resources and Earth sciences High resolution imagery, digital photography
ISS	322 (LEO)	Space science and technology
Generic GEO	GEO	Remote sensing
Generic HEO	HEO	Launch detection and other

It is emphasized that these events were chosen only for purposes of effects analysis. The satellites (**table 10-2**) were chosen to be representative of the many types and missions in orbit and to be representative targets for the radiation effects.

### **Prompt Radiation Effects**

When a weapon is detonated at high altitude, satellites that lie within line of sight of the burst will be subject to direct (X-ray) radiation. Satellites in the shadow cast by the Earth will not be directly irradiated, as illustrated in **figure 10-3**, but will be subject to electron radiation as they transit debris and decay-products (primarily energetic beta electrons) mentioned previously that are trapped in the Earth's magnetic field. If there is a significant mass of intervening atmosphere between the detonation point and the satellite, direct nuclear radiation will be attenuated. Lacking this intervening shield, the radiation fluence will decrease as the inverse square of the distance.

Worst-case situations occur when a satellite is nearest the burst; for example, directly above or below it. In such cases, the range between satellite and burst is minimized, and X-ray, gamma, and neutron fluences on the satellite are maximized. Full evaluation of this hazard requires statistical analysis. The likelihood that the satellite will be in direct line of sight of the burst is typically 5 to 20 percent, depending on orbital parameters for the satellite and burst location. Even then, damage may be ameliorated by either distance or intervening atmosphere.

Calculations of X-ray exposure probabilities were performed for Events 9, 13, 17, and 18. The calculations yield the probability that a specific satellite will be exposed to a specified level of X-ray fluence. Results appear in **table 10-3**. With this information, one can estimate the probability of satellite damage based on known damage thresholds for spacecraft materials. Thresholds for various types of damage were chosen at, or close to, values accepted by the engineering community. Here, thermomechanical damage refers to removal or degradation of the coatings on solar cell surfaces. Depending on nuclear weapon output spectra, coating damage is generally a satellite's most sensitive thermomechanical damage mode. SGEMP (System-Generated EMP) burnout is damage caused by currents associated with X-ray-induced electron emission. Latch-up is a logic state setting of a semiconductor device that becomes frozen as a result of radiation exposure. Latch-up may cause large currents to flow in the affected circuit, resulting in unacceptable current-induced damage (i.e., burnout).

Line-of-sight exposure of the ISS to photons can cause significant damage to the solar-array coverglass coatings for Events 6, 7, 8, 9, and 17. NOAA/DMSF and TERRA/IKONOS are unlikely to be promptly affected thermomechanically by a line-of-sight



photon exposure in any of our postulated nuclear events. Satellites in GEO are sufficiently far away because of their higher altitudes that the inverse square fall-off of the radiation reduces the potential exposure to a tolerable level.

**Table 10-3. Probability That Satellites Suffer Damage by Direct Exposure to X-Rays**

Satellite	Event	Probability of damage due to thermomechanical damage (%)	Probability of damage due to SGEMP/burnout (%)	Probability of damage due to latch-up/burnout (%)
ISS	9	1.7	4	4.2
	18	0	5	5
	13	~ 0	3	4
	17	1.7	5	5
NOAA	18	0.2	19	20
	13	0	3	5
	17	1	7	8
TERRA	18	~ 0.3	18	18
	13	0	2	5
	17	1.2	7	7

### ***Permanent Damage from Exposure to the Enhanced Electron Belts***

For this report, nuclear-enhanced electron belts are modeled as though they were providing a relatively constant trapped-electron environment. **Tables 10-4, 10-5, and 10-6** display reduced lifetimes of satellites that result from 17 of the 21 events. Results of events 18 through 21 will be discussed below.

**Table 10-4. Trial Events in Group 1**

Event	Yield (kT)	HOB (km)	Time to Failure (days)		
			NOAA	TERRA	ISS
1	20	200	30	70	150
2	100	175	15	30	50
3	300	155	4	7	9
4	10	300	20	60	5,400
5	100	170	30	70	100

Reduction in satellite lifetime is based on total dose from higher energy electrons to internal electronics, assumed to be shielded by a 0.100-inch slab of aluminum. In evaluating the biological response of astronauts to radiation on the ISS, 0.220 inches of slab shielding was assumed because the astronauts would usually be inside the pressurized modules of the space station. Some critical electronics for the station were still assumed to be shielded by only 100 mils of aluminum. Satellites are assumed to be hardened to twice the long-term-average natural background radiation encountered during a nominal mission.<sup>10</sup> Just as with photons, damage to spacecraft thermal, optical, and other surface coatings is caused by exposure to electrons of relatively low energies.

Except for the ISS in Event 4, even the low-yield events are capable of imposing a much-reduced lifetime on the satellites.

In the set of events depicted in **table 10-5**, the large weapon used in Event 17 inflicts severe damage on the ISS. Significantly, this exposure would cause radiation sickness to the astronauts within approximately 1 hour and a 90 percent probability of death within 2 to 3 hours.

<sup>10</sup> While the use of twice the expected long-term-average exposure as a gauge of lifetime, as discussed here, is common practice, it relies entirely on total dose as a measure of radiation tolerance and ignores dose rate effects. Risks from circumstances involving nuclear detonations, where dose rates could be much larger than encountered under natural conditions, may be underestimated.

Events 6 through 11 (**table 10-6**) were chosen within a geographical region where satellites could be placed at risk from a direct EMP attack resulting from regional contingencies.

**Table 10-5. Trial Events in Group 2**

Event	Yield (kT)	HOB (km)	Time to Failure (days)		
			NOAA	TERRA	ISS
12	20	150	25	60	230
13	100	120	60	200	200
14	500	120	4	6	3
15	100	200	10	20	30
16	500	200	1	3	4
17	5,000	200	0.1	0.1	0.1

**Table 10-6. Trial Events in Group 3**

Event	Yield (kT)	HOB (km)	Time to Failure (days)		
			NOAA	TERRA	ISS
6	800	368	1	1	0.5
7	800	491	1	1	1
8	4,500	102	0.1	0.2	0.2
9	4,500	248	0.1	0.2	0.2
10	30	500	40	100	150
11	100	200	10	17	20

The results of weapons detonated at high latitudes (Events 18 through 21) produced no dramatic nuclear effects. This is largely because these satellites are designed to operate in a far more hostile natural space environment due to the solar wind than are those in LEO.

Generally, most papers dealing with satellite lifetimes following a high-altitude nuclear detonation treat radiation effects on newly launched satellites with no pre-burst accumulated total dose. Except for satellites launched as replacements after a detonation, a more realistic assessment would assume a high-altitude detonation after a satellite had been in orbit for a portion of its anticipated service life. If a satellite is near the end of its design lifetime (i.e., has accumulated the majority of the total dose it can tolerate) prior to the detonation, the dose absorbed from a nuclear-pumped belt could cause prompt demise. To evaluate potential life-shortening effects on satellites, we examined a constellation of generic satellite systems. To assess sensitivity to assumed hardening level, we evaluated two hypothetical constellations. One constellation was assumed hardened to 1.5 times the natural total dose anticipated over the design lifetime (1.5x). The other constellation was assumed hardened to 2x. The scenario involved a 10 MT burst (50 percent fission yield) detonated on May 23, 2003, at an altitude of 90 km over northern Lake Superior (48.5 degrees north latitude, 87 degrees west longitude). Total dose for each constellation was based on realistic code calculations.

**Figure 10-6** shows the resulting number of satellites remaining as a function of time after the burst. The blue and red curves correspond to the constellations hardened to 1.5x and 2x, respectively. Corresponding outage times for ground-based receivers are shown in **Figure 10-7**. Clearly, decreasing satellite hardening by 25 percent has a marked effect on survivability in this case.

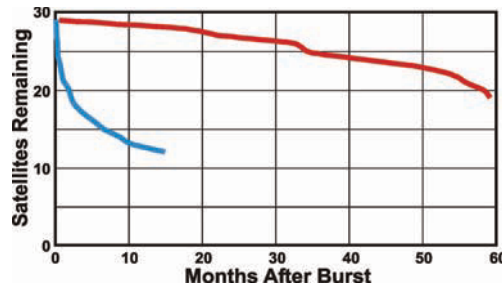


Figure 10-6 . Satellites remaining after a 10 MT burst over Lake Superior



Figure 10-7. Satellite ground-based receiver outage time after a 10 MT burst over Lake Superior

HEO satellites already reside in orbits that are relatively challenging in terms of the natural radiation environment. Assuming these satellites are hardened to twice the natural dose they would normally accumulate in 15 years, a satellite's electronics would be hardened to approximately 325 krad behind a 100 mil (0.1 inch) semi-infinite slab of aluminum. With this level of hardness, one would expect that these satellites would not be vulnerable to a high-altitude burst of a single, low-yield (approximately 50 kT) device of unsophisticated design. Realistic code calculations suggest this is indeed the case.

Three large-yield events were investigated to determine whether they would present a threat to HEO satellites. Two of these events (Events 11 and 21) would not present a total ionizing dose problem for the satellite. Although Event 21 is a 10-MT burst, it has little effect on a HEO satellite because the trapped electrons are spread out over a large L-shell region. In contrast, the 100 kT of Event 11 does result in some detectable radiation accumulation on the satellite as it passes through altitudes near perigee. The yield is, however, too low to present a threat to the satellite. A 5-MT burst depicted in Event 17, on the other hand, does present a substantial threat to HEO satellites, given the hardening assumptions mentioned earlier. **Figure 10-8** shows that the assumed 2x natural hardening level of the satellite is exceeded about 36 days after Event 17.

Analysis of direct EMP attacks over the northern continental United States (CONUS) or Canada indicates lesser risk to LEO satellites from weapons with yields ranging from 10 kT to 100 kT. For yields approaching 1 MT (or greater) detonated at such latitudes, it becomes more difficult to predict the fate of LEO satellites. The larger yields make more severe nuclear-enhanced trapped flux environments, but depletion rates of trapped fluxes (both natural and nuclear) are difficult to predict.

### Satellite Ground Stations

Although bursts over CONUS may not directly damage satellites, the EMP effect on ground control stations could still render some satellites inoperable. We have focused our analyses on collateral weapon effects on satellites, without discussion of EMP effects on ground stations used for uplinks, downlinks, and satellite control. Currently, many of the

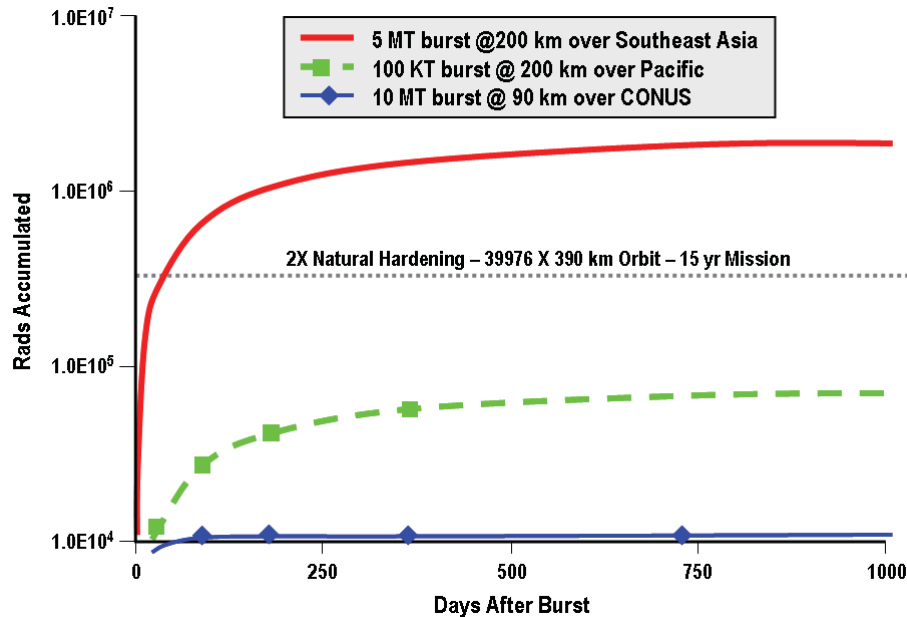


Figure 10-8. HEO satellite exposure to trapped radiation produced by Events 11, 17, and 21

important satellite systems use unique transmission protocols with dedicated ground terminals. Unique protocols limit interoperability, so loss of dedicated ground terminals could readily compromise overall functionality of a system, even if the system's satellites remained undamaged.

While satellites generally are designed to operate autonomously, with periodic house-keeping status downloads to ground controllers and uploads of commands, once damaged, satellites may require frequent, perhaps continuous, control from the ground to remain even partially functional. Thus, loss of ground stations to EMP could render otherwise functional satellites ineffective or lead to premature loss.

A comprehensive analysis of overall satellite system degradation should include potential loss of ground stations and cost/benefit trade-offs with respect to EMP hardening. A scenario-based analysis would reveal the extent to which loss of individual ground stations may pose an additional level of vulnerability.

## Discussion of Results

Given inherent satellite fragility owing to severe weight constraints, any nation with missile lift capability and sufficient technology in the requisite disciplines can directly attack and destroy a satellite. Such attacks are outside the focus of this study. The Commission considered only hazards to satellites that may arise as collateral nuclear weapon effects during an EMP attack. The prominent collateral hazards are prompt nuclear output (X-rays, gamma rays, and neutrons), high fluences of UV photons generated by some high-altitude nuclear detonations, and nuclear burst enhancement (pumping) of the radiation belts surrounding the Earth in the region of space where satellites orbit.

The worst-case exposure of a satellite to direct x-radiation from a nuclear weapon can be lethal. For LEO satellites, the threat can be nonnegligible, but for satellites at GEO, the large distance between a detonation designed for an EMP attack and a satellite makes the probability of direct damage very low. The same argument holds for exposure to gamma rays, neutrons, and burst-generated UV light.

Nuclear-enhanced radiation belts must be considered differently, owing to their persistence and wide spatial distribution around the Earth. Because the natural trapped radiation environment at GEO is more severe on average than at most LEO locations, satellites at GEO typically are hardened to a greater extent than LEO satellites. Absent large yields (megatons), burst-generated energetic electron fluxes trapped in high-latitude (i.e., high L-shell) magnetic flux tubes generally are not sufficiently intense and long-lasting to cause the early demise of satellites in GEO, unless those satellites have accumulated sufficient natural radiation exposure to put them near the end of their service lives.<sup>11</sup>

Satellites in LEO are much more susceptible to damage from both direct and persistent radiation that results from an EMP attack, but the possibility of damage is highly dependent on weapon parameters (latitude and longitude, height of burst [HOB], and weapon yield).

Line-of-sight exposure of LEO research satellites such as ISS to X-ray and UV photons can cause significant damage to solar-array coverglass coatings for Events 6, 8, 9, 17, and 19. While such exposures are statistically infrequent, in those instances where they occur, they will result in immediate loss of many operational capabilities, as well as loss of power generating capacity.

The low-energy component of trapped-electron flux from beta decay of fission products and decay of free neutrons exceeds the long-term average natural flux for the high-yield Events 8, 9, and 17. Such flux levels will cause electrostatic breakdown in certain types of thermal radiator coatings and external cables on NOAA and TERRA within the first few days following the burst.

### ***Uncertainties in Estimates***

Uncertainties in satellite vulnerabilities result from imprecise knowledge of threat environments, combined with uncertainties in responses of satellite materials to those environments. Difficulties in characterizing aging effects of materials exposed to on-orbit conditions for extended periods exacerbate these uncertainties.

In the following comments, it is assumed that the weapons in question mirror U.S. technology available in the time frame 1970 to 1980.

Uncertainties in direct line-of-sight exposure of a satellite to radiation from a nuclear detonation result primarily from unknowns associated with the design of an offensive weapon, its delivery system, and its detonation altitude. These factors determine the fraction of weapon yield emitted as photons, neutrons, and beta particles and, hence, the type and magnitude of damage they inflict on satellites. Variability of weapon designs is estimated to lead to an uncertainty of approximately plus or minus a factor of five in UV hazard source strength (radiation primarily emitted from a weapon's case and its packaging within a delivery vehicle [but see below for more on UV photons]). Based on computational correlations with experimental data, there exists at least a factor of 10 uncertainty in X-ray spectral intensity at arbitrary photon energies of a kilovolt or more. Uncertainties in gamma-ray fluence and flux predictions are thought to be on the order of  $\pm 15$  percent, as are those for prompt neutrons. Total yield is believed to be accurate to  $\pm 10$  percent.

---

<sup>11</sup> The reader is reminded that our analysis deals only with collateral damage resulting from an EMP attack. Direct attack on satellites at any altitude, though serious, is not within the bounds of this analysis.



For bursts below a few hundred kilometers altitude, the debris-air blast-wave-generated fluence of UV photons (which can be as large as 80 percent of the kinetic yield of the device) carries an estimated uncertainty factor of 3 to 10, depending primarily on device characteristics. These uncertainty factors are ameliorated to some degree by decreasing burst altitude. Detonations below approximately 90 km occur in sufficiently dense air that UV photons are largely absorbed before they can escape to space.

Uncertainties in trapped radiation environments from high-altitude nuclear detonations also result from unknowns in offensive weapon design, but additional uncertainties arise in dispersal of radioactive weapon debris, efficiency with which beta particles become trapped in the geomagnetic field, subsequent transport of trapped particles, and the rapidity with which nuclear-burst enhancements of the radiation belts decay into the natural background. Under the best of circumstances, uncertainties in the intensity and persistence of trapped radiation estimated for the events considered in this report are at least a factor of 10 and are likely substantially more in situations that depart from limited circumstances of past nuclear tests.

## Findings

### ***Potential Vulnerabilities***

An EMP attack on any of several important geographic regions could cause serious damage to LEO satellites. The STARFISH high-altitude nuclear burst greatly enhanced the high-energy electron environment in LEO, resulting in the early demise of several satellites on orbit at the time.<sup>12</sup> Copious documentation exists that describes recent radiation-induced satellite failures due to the natural radiation environment alone.

Given the large uncertainties discussed above, there may be a temptation to ignore the issue of high-altitude nuclear threats to satellites for the time being simply because insufficient information is available to implement a cost-effective protection solution. We believe that ignoring the issue would be ill advised for a number of reasons, including the consequences of losing possibly tens of billions of dollars in LEO space assets in a short time.

### ***Mitigation of Threats***

Any adversary possessing a lift and orbiting control capability can destroy a satellite: it is clearly neither cost effective nor desirable to harden every satellite against every possible threat. The challenge is to weigh risks/rewards of mitigation against mission priorities and plausible threats. A number of threat mitigation measures exist or have been proposed as an alternative or supplement to hardening.

Any combination of hardening and mitigation options can be chosen to achieve the required degree of survivability. Alternatives must be explored, documented, and reviewed so that management and users of space assets can make rational appraisals of the costs, benefits, and consequences of space system degradation and/or loss.

### ***Hardening of Satellites and Ground Stations***

Commercial satellites are hardened against their natural orbital environment to achieve the lifetime necessary to realize a profit. The technology to accomplish this goal is built into their design and factored into their cost. Protection from nuclear threats is not

---

<sup>12</sup> Weenas, E.P., "Spacecraft Charging Effects on Satellites Following STARFISH Event," RE-78-2044-057, February 17, 1978.

provided to commercial satellites because, from the commercial operator's perspective, it is not cost effective to do so.

The cost of hardening a system has been a subject of continuing controversy for the past 45 years. Systems project offices tend to estimate high to avoid the introduction of measures that threaten to escalate system cost. Achievable cost control is contingent upon ab initio design of radiation hardness into the system rather than on retrofitting it. Options other than hardening and shielding include repositioning selected satellites in times of stress to minimize exposure to enhanced radiation belts.

If the ground stations for satellites in any orbit are not hardened to EMP, the utility of the satellites could degrade, depending on their ability to operate autonomously.

### **Recommendations**

- ◆ Each Federal Government organization that acquires and/or uses space should execute a systematic assessment of the significance of each such space system, particularly those in low Earth orbits, to its missions. Information from this assessment and associated cost and risk judgments will inform senior government decision-making regarding protection and performance assurance of these systems, so that each mission can be executed with the required degree of surety in the face of possible threats.

## Chapter 11. Government

### Introduction

A primary role of the Federal Government is to defend the Nation against threats to its security. EMP represents one such threat. Indeed, it is one of a small number of threats that can hold our society at risk of catastrophic consequences. The Executive branch of the Federal Government bears the responsibility for executing a strategy for dealing with this threat. The Commission has recommended a strategy for addressing this threat that combines prevention, protection, and recovery. It represents what we believe to be the best approach for addressing the EMP threat.

The Commission has identified an array of recommendations relating to civilian infrastructures that are logical outgrowths of our recommended strategy. Those recommendations relating to civilian infrastructures are contained in the individual chapters of this volume and will not be repeated here. Implementation of these recommendations will result in the identification of responsibilities at the regional, state, and local levels.

The Federal Government not only has the responsibility for being appropriately postured to cope with all aspects of the EMP threat, including preparations for recovery, but also has the responsibility to be able to respond to and manage national recovery in a competent and effective manner in the wake of an EMP attack. American citizens expect such competence and effectiveness from responsible government officials at all levels. In order to properly manage response and recovery, essential government functions will have to survive and function in the wake of an EMP attack.

### Maintaining Government Connectivity and Coherence

It is essential that the Government continues to function through an electromagnetic pulse (EMP) emergency. Events over the last few years have highlighted the need for assured and real-time communications connectivity between government leadership and organizational assets for both crisis management and the management of a controlled recovery. Plans to ensure the continued functioning of government are embodied in Continuity of Operations (COOP) plans prepared by government organizations in anticipation of emergency situations and Continuity of Government (COG) planning to ensure the survival of constitutional government. National Security Presidential Directive 51 (NSPD 51) and Homeland Security Presidential Directive 20 (HSPD 20 on the subject of “National Continuity Policy”, as described in a White House summary released May 9, 2007<sup>1</sup>), outlines these issues and directs the implementation of COOP and COG (excerpts noted below). The EMP Commission met with National Security Council staff to discuss COG-related issues as they might relate to EMP threats. However, COG planning remains highly classified, and only this top-level overview can be provided within this venue.

### Recommendations

- ◆ The Department of Homeland Security (DHS) should give priority to measures that ensure the President and other senior Federal officials can exercise informed leadership of the Nation in the aftermath of an EMP attack and that improve post-attack response capabilities at all levels of government.

---

<sup>1</sup> National Security and Homeland Security Presidential Directive,  
<http://www.whitehouse.gov/news/releases/2007/05/20070509-12.html>.

- ◆ The President, Secretary of Homeland Security, and other senior officials must be able to manage national recovery in an informed and reliable manner. Current national capabilities were developed for Cold War scenarios in which it was imperative that the President have assured connectivity to strategic retaliatory forces. While this requirement is still important, there is a new need for considerably broader and robust connectivity between national leaders, government at all levels, and key organizations within each infrastructure sector so that the status of infrastructures can be assessed in a reliable and comprehensive manner and their recovery and reconstitution can be managed intelligently. The DHS, working through the Homeland Security Council, should give high priority to identifying and achieving the minimum level of robust connectivity needed for recovery following an EMP attack. In doing so, DHS should give particular emphasis to exercises that evaluate the robustness of the solutions being implemented.
- ◆ Working with state authorities and private sector organizations, the DHS should develop draft protocols for implementation by emergency and other government responses following an EMP attack, Red Team these extensively, and then institutionalize validated protocols through issuance of standards, training, and exercises.

***NSPD 51/HSPD 20***  
***Subject: "National Continuity Policy"***  
***9 May 2007***

**Purpose**

(1) This directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies. This policy establishes "National Essential Functions," prescribes continuity requirements for all executive departments and agencies, and provides guidance for State, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

**Definitions**

(2) In this directive:

(a) "Category" refers to the categories of executive departments and agencies listed in Annex A to this directive;

(b) "Catastrophic Emergency" means any incident, regardless of location, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the U.S. population, infrastructure, environment, economy, or government functions;

(c) "Continuity of Government," or "COG," means a coordinated effort within the Federal Government's executive branch to ensure that National Essential Functions continue to be performed during a Catastrophic Emergency;

(d) "Continuity of Operations," or "COOP," means an effort within individual executive departments and agencies to ensure that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies;

(e) "Enduring Constitutional Government," or "ECG," means a cooperative effort among the executive, legislative, and judicial branches of the Federal Government, coordinated by the President, as a matter of comity with respect to the legislative and judicial branches and with proper respect for the constitutional separation of powers among the branches, to preserve the constitutional framework under which the Nation is governed and the capability of all three branches of government to execute constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, and interoperability and support of the National Essential Functions during a catastrophic emergency;

(f) "Executive Departments and Agencies" means the executive departments enumerated in 5 U.S.C. 101, independent establishments as defined by 5 U.S.C. 104(1), Government corporations as defined by 5 U.S.C. 103(1), and the United States Postal Service;

(g) "Government Functions" means the collective functions of the heads of executive departments and agencies as defined by statute, regulation, presidential direction, or other legal authority, and the functions of the legislative and judicial branches;

(h) "National Essential Functions," or "NEFs," means that subset of Government Functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP and COG capabilities; and

(i) "Primary Mission Essential Functions," or "PMEFs," means those Government Functions that must be performed in order to support or implement the performance of NEFs before, during, and in the aftermath of an emergency.

**Policy**

(3) It is the policy of the United States to maintain a comprehensive and effective continuity capability composed of Continuity of Operations and Continuity of Government programs in order to ensure the preservation of our form of government under the Constitution and the continuing performance of National Essential Functions under all conditions.



**Implementation Actions**

(4) Continuity requirements shall be incorporated into daily operations of all executive departments and agencies. As a result of the asymmetric threat environment, adequate warning of potential emergencies that could pose a significant risk to the homeland might not be available, and therefore all continuity planning shall be based on the assumption that no such warning will be received. Emphasis will be placed upon geographic dispersion of leadership, staff, and infrastructure in order to increase survivability and maintain uninterrupted Government Functions. Risk management principles shall be applied to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences.

...

(10) Federal Government COOP, COG, and ECG plans and operations shall be appropriately integrated with the emergency plans and capabilities of State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to promote interoperability and to prevent redundancies and conflicting lines of authority. The Secretary of Homeland Security shall coordinate the integration of Federal continuity plans and operations with State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to provide for the delivery of essential services during an emergency.

(11) Continuity requirements for the Executive Office of the President (EOP) and executive departments and agencies shall include the following:

(a) The continuation of the performance of PMEFS during any emergency must be for a period up to 30 days or until normal operations can be resumed, and the capability to be fully operational at alternate sites as soon as possible after the occurrence of an emergency, but not later than 12 hours after COOP activation;

(b) Succession orders and pre-planned devolution of authorities that ensure the emergency delegation of authority must be planned and documented in advance in accordance with applicable law;

(c) Vital resources, facilities, and records must be safeguarded, and official access to them must be provided;

(d) Provision must be made for the acquisition of the resources necessary for continuity operations on an emergency basis;

(e) Provision must be made for the availability and redundancy of critical communications capabilities at alternate sites in order to support connectivity between and among key government leadership, internal elements, other executive departments and agencies, critical partners, and the public;

(f) Provision must be made for reconstitution capabilities that allow for recovery from a catastrophic emergency and resumption of normal operations; and

(g) Provision must be made for the identification, training, and preparedness of personnel capable of relocating to alternate facilities to support the continuation of the performance of PMEFS.

...

(19) Heads of executive departments and agencies shall execute their respective department or agency COOP plans in response to a localized emergency and shall:

(a) Appoint a senior accountable official, at the Assistant Secretary level, as the Continuity Coordinator for the department or agency;

(b) Identify and submit to the National Continuity Coordinator the list of PMEFS for the department or agency and develop continuity plans in support of the NEFs and the continuation of essential functions under all conditions;

(c) Plan, program, and budget for continuity capabilities consistent with this directive;

(d) Plan, conduct, and support annual tests and training, in consultation with the Secretary of Homeland Security, in order to evaluate program readiness and ensure adequacy and viability of continuity plans and communications systems; and

(e) Support other continuity requirements, as assigned by category, in accordance with the nature and characteristics of its national security roles and responsibilities

...

GEORGE W. BUSH

## Chapter 12. Keeping The Citizenry Informed: Effects On People

### Introduction

The best current estimate is that the electromagnetic pulse (EMP) produced by a high-altitude nuclear detonation is not likely to have direct adverse effects on people. Such effects have not been observed for the personnel who operate EMP simulators.<sup>1</sup> Medical surveillance studies on human exposure to pulsed electromagnetic fields have supported this inference.<sup>2</sup>

An important exception is people whose well-being depends on electronic life support equipment. They will be directly impacted by effects that disrupt or damage such devices. Research sponsored by the Commission suggests that some heart pacemakers may be among the devices susceptible to upset from high-altitude EMP.<sup>3,4</sup>

While most effects on people would be indirect, they could be significant in a just-in-time economy in which local stocks of medicines, baby food, and other health-critical items are limited. The physical consequences of the serious high-altitude EMP attacks on the United States (U.S.) of concern to the Commission would likely include the failure of the electric power grid and degradation of telecommunication systems, computers, and electronic components over large areas of the country. A disruption of this scale could cripple critical infrastructures and hinder the delivery of day-to-day necessities, because of the interconnectivity of telecommunication networks and the electrical dependence of most cities, government agencies, businesses, households, and individuals. It also could require a long recovery period. To assess human consequences, the contingency of concern is one in which electricity, telecommunications, and electronics are out of service over a significant area for an extended period of time.

The human consequences of such a scenario include the social and psychological reactions to a sudden loss of stability in the modern infrastructure over a large area of the country. Loss of connectivity between the government and its populace would only exacerbate the consequences of such a scenario.

This analysis is based largely on selected case studies, including major blackouts, natural disasters, and terrorist incidents in recent U.S. history. These incidents served as approximate analogs in order to best predict the sociological and psychological effects of an EMP attack.

### Impact of an EMP Attack

While no single event serves as a model for an EMP scenario with incidence of long-lasting widespread power outage, communications failure, and other effects, the combined analysis of the following case studies provides useful insight in determining human reactions following an EMP attack:

Blackouts:

- ◆ Northeast (1965)
- ◆ New York (1977)

---

<sup>1</sup> Patrick, Eugene L., and William L. Vault, *Bioelectromagnetic Effects of the Electromagnetic Pulse (EMP)*, Adelphi, MD: Harry Diamond Laboratories, March 1990, pp. 6–7.

<sup>2</sup> Ibid, pp. 8–10.

<sup>3</sup> EMP Commission Staff Paper, Quick Look Pacemaker Assessment, December 2003.

<sup>4</sup> Sandia National Laboratory, EMP Commission-sponsored test.

- ◆ Hydro Quebec (1989)
- ◆ Western states (1996)
- ◆ Auckland, New Zealand (1998)
- ◆ Northeast (2003)

Natural Disasters:

- ◆ Hurricane Hugo (1989)
- ◆ Hurricane Andrew (1992)
- ◆ Midwest floods (1993)

Terrorist Incidents:

- ◆ World Trade Center attack (2001)
- ◆ Anthrax attacks (2001)

### **Blackouts**

In 1965, a blackout occurred over the northeastern United States and parts of Canada. New Hampshire; Vermont; Massachusetts; Connecticut; Rhode Island; New York, including metropolitan New York City; and a small part of Pennsylvania were in the dark after operators at Consolidated Edison were forced to shut down its generators to avoid damage. Street traffic was chaotic, and some people were trapped in elevators, but there were few instances of antisocial behavior while the lights were out.<sup>5</sup> It was a “long night in the dark,” but the recovery proceeded without incident, and citizens experienced relative civility.

*TIME* Magazine described New York’s next blackout, in 1977, as a “Night of Terror.”<sup>6</sup> Widespread chaos reigned in the city until power was restored — entire blocks were looted and set ablaze, people flipped over cars and vans on the streets; the city was in pandemonium. That night 3,776 arrests were made, and certainly not all looters, thieves, and arsonists were apprehended or arrested.<sup>7</sup> While this is a dramatic example of antisocial behavior following a blackout, sociologists point to extraordinary demographic and historical issues that contributed to the looting. For instance, extreme poverty and socio-economic inequality plagued New York neighborhoods, and many of the looters originated from the poorer sections of the city, engaging in “vigilante redistribution” by looting consumer goods and luxuries. Racial tensions were high, and a serial killer known as Son of Sam had recently terrorized New Yorkers.

In 1989, more than 6 million customers lost power when the geomagnetic storm discussed in Chapter 4 caused a massive power failure in Quebec. The electricity failures caused by this geomagnetic storm reached a much larger area than is typically affected by traditional blackouts resulting from technological failure. However, the outage lasted just over 9 hours, most of which were during the day.<sup>8</sup> The local and national papers were curiously silent about the blackout, and little to no unusual or adverse human behavior was attributed to the power loss. The event was most significantly a lesson for operators of the North American electric grids because it revealed vulnerabilities in the system.

<sup>5</sup> “The Great Northeast Blackout of 1965,” <http://www.ceet.niu.edu/faculty/vanmeer/outage.htm>.

<sup>6</sup> Sigwart, Charles P., “Night of Terror,” *Time*, July 25, 1977.

<sup>7</sup> “1977 New York Blackout,” Blackout History Project, <http://blackout.gmu.edu/events/tl1977.html>.

<sup>8</sup> Kappenman, John G., “Geomagnetic Storms Can Threaten Electric Power Grid,” *Earth in Space*, Vol. 9, No. 7, March 1997, pp.9-11. © 1997 American Geophysical Union. [http://www.agu.org/sci\\_soc/eiskappenman.html](http://www.agu.org/sci_soc/eiskappenman.html).

In 1998, Auckland, New Zealand, experienced a significant blackout that lasted more than 5 weeks and affected more than 1 million people.<sup>9</sup> Civility reigned for the duration of the outage, which was likely attributed to a number of factors, including:

- ◆ There was no significant threat to public health, because water and sewage infrastructures were functioning.
- ◆ In anticipation of potential incidents, police increased their presence in urban areas.
- ◆ The recovery process was underway nearly immediately, communicating to the public that the situation would eventually be under control.
- ◆ Nearly all blackout recovery resources of New Zealand were rushed to the capital for recovery efforts.

Recovery efforts from elsewhere in New Zealand were significant symbolically as well as practically, as demonstrated by the fact that electricity was available elsewhere. Businesses attempted to carry on as normally as possible, with some examples of opportunism, such as businesses relocating to more desirable spaces that had been vacated. Social consequences included criticism and blame of the authorities, both municipal and national, because the technological failures were attributed in large part to privatization of the power sector. However, this response never materialized into violence, crime, or social disorder.

Most recently, New York City and the eight states in the northeast experienced another significant blackout in August 2003. While the blackout inconvenienced many on a hot summer day, general civility remained intact. News coverage indicated that those affected by the blackout dealt with the obstacles quietly and even developed a sort of camaraderie while struggling through nights without running water and electricity. In contrast to the 1977 blackout, police made only 850 arrests the night of the 2003 blackout, of which “only 250 to 300 were directly attributable to the blackout,” indicating a slight decline from the average number of arrests on a given summer day.<sup>10</sup> While this blackout was widespread, it was not long lasting, and it did not interrupt the communications infrastructure significantly.

Blackouts provide only a partial picture of life following an EMP attack. Most blackouts are localized and are resolved quickly. Further, usually communication systems are not completely shut down, and major infrastructures can remain intact if significant portions of infrastructure hardware are located outside of the affected area. In order to best approximate the effects of longer-lasting, widespread infrastructure disruption—with or without electrical power failure—it is necessary to look to natural disasters for examples of human reaction.

### **Natural Disasters**

At the time that Hurricane Hugo hit in 1989, it was the most intense hurricane to strike Georgia and the Carolinas in 100 years. Surveys of Hurricane Hugo’s survivors indicate that some individuals who suffered personal and financial losses from the hurricane showed clinically significant symptoms of psychological trauma. According to some researchers, many of the adverse mental health effects of Hugo could be explained by deterioration in perceived social support. While on the whole, the rate of post-traumatic

<sup>9</sup> “Power failure brings New Zealand’s largest city to standstill,” CNN, <http://www.cnn.com/WORLD/9802/24/nzealand.blackout/index.html>.

<sup>10</sup> Adler, Jerry, et al, “The Day the Lights Went Out,” *Newsweek*; August 25, 2003, Vol. 142, Issue 8, p. 44.

stress disorder symptoms was low, stress effects lingered long after the hurricane's physical damage was repaired.

Hurricane Andrew blew through the southeastern United States and along the coast of the Gulf of Mexico in 1992, causing \$26.5 billion in damage. Andrew left 250,000 families homeless and 1.4 million families without electricity immediately following the hurricane. After such extraordinary destruction and disruption, it is perhaps not surprising that one-third of a sample of individuals met criteria for post-traumatic stress disorder 4 months after the hurricane.<sup>11</sup>

Hurricanes Hugo and Andrew demonstrated to psychologists that disaster-related declines in perceived support explained the difference in symptoms between the two disasters; deterioration was more significant in Andrew and recovery was weaker. In the long-lasting recovery period, Floridians saw looting, opportunism, and vigilante civil defense. Press coverage of Hurricane Andrew suggests that after a multi-state disaster, people will expect help, and they will expect it from the federal government, as well as from state and local authorities.

Flooding in the American Midwest in 1993 resulted in 25 deaths, affected more than 8 million acres, and cost billions of dollars in property damage and more than 2 billion dollars in crop damage. Water depths ranged from 11 feet of flooding in Minneapolis to 43 feet in St. Louis. Electricity was restored where possible within 3 days and in downtown Des Moines within 23 hours. The floods devastated families, businesses, and individuals, who lost nearly everything and were unable to control events throughout the recovery process. Thousands of people assisted in volunteer recovery efforts by sandbagging and providing needed supplies.<sup>12</sup> Most came from unaffected areas to help the most urgent victims. The floods provide an example of widespread damage crippling several infrastructures for a significant period of time and an example of a disaster in which regional experience may matter tremendously in disaster recovery.

Blackouts and natural disasters have limits as approximations of recovery following an EMP attack. An important element is the relevance of fear and individual panic in these situations versus what might occur following an EMP attack. For this component, it is useful to examine recent terrorist incidents in the United States in order to gauge the effects of fear among the public. Because terrorist attacks appear to be indiscriminate and random, they can arouse acute anxiety and feelings of helplessness, which shatter beliefs of invulnerability and even a belief in justice and order in the world.

### **Terrorist Incidents**

The attacks on the World Trade Center in New York on September 11, 2001, certainly qualified as seemingly indiscriminate and random. Following this disaster, in which nearly 3,000 people died, those in the immediate and surrounding area showed considerable psychological trauma and damage. Some individuals who experienced these attacks may have lost confidence in their abilities to cope and control outcomes. Overall, however, the survivors of the attacks proved remarkably resilient, flexible, and competent in the face of an arbitrary, violent, and completely unexpected attack.<sup>13</sup>

---

<sup>11</sup> Norris, et al, "60,000 Disaster Victims Speak: Part 1. An Empirical Review of the Empirical Literature, 1981-2001," *Psychiatry*, Fall 2002, 65, 3, Health Module.

<sup>12</sup> Barnes, Harper, "The Flood of 1993," *St. Louis Post-Dispatch*, July 25, 1993.

<sup>13</sup> Kendra, James, and Tricia Wachtendorf, "Elements of Resilience in the World Trade Center Attack," Disaster Research Center, 2001.



In October 2001, a month following the attack on the World Trade Center, Americans saw a series of anthrax-infected mail pieces threatening intended mail recipients and handlers. The death toll was small (five individuals), but public concern was considerable. This period is an example of public response to an adversary-initiated threat that disrupted infrastructure. The public demonstrated a great need for control over the situation, through preparedness and information. For example, many Americans took protective measures, despite the astronomical odds against infection. The news media were saturated with reports of anthrax infections, suspected infections, and general information about anthrax and how to respond to infection. Though no culprit was apprehended, the attacks stopped, and normal postal activity resumed.

### ***Some Lessons Learned***

Though the United States has not experienced a severe, widespread disruption to infrastructure comparable to an EMP attack, the cases reviewed provide some practical direction for predictions of behavior. For example, it can be expected that emotional reactions such as shock and paralysis that have followed past disasters could be magnified in a large-scale event such as an EMP attack. In particular, the paralysis of government assistance entities, such as law enforcement and emergency services, would aggravate this effect. In most instances, social disorder would be minimal, in significant part, due to the knowledge that authorities are in control of the situation. Without that assurance from an outside source, it appears likely that people would turn to immediate neighbors or community members for information and support, if possible.

Following disruptive disasters, information is among the most pressing needs for individuals. Not surprisingly, people's first concerns are the whereabouts and safety of their family members and friends. Another urgent priority is an understanding of the situation — knowledge of what has happened, who and what is affected, and the cause of the situation. A related yet distinct information need is for confirmation that the situation will be resolved, either from common sense and experience, in the case of a small-scale disaster, or from the involvement of local or federal authorities, in the case of a large-scale disaster. Psychologists note that dramatic events force people to reexamine their basic understanding about the world, and that survivors need to process an event before they can fully absorb it. This information processing begins the alternating phases of intrusion and avoidance that are primary indicators of post-traumatic stress.<sup>14</sup>

The aftermath of natural disasters is often marked by instances or a period of considerable pro-social behavior such as cooperation, social solidarity, and acts of selflessness. However, this encouraging observation might not be similarly magnified in projections for human behavior following an EMP attack. The key intangible, immeasurable difference is the knowledge that normal order would resume, based on significant indicators.

It is important to note some of the differences between natural disasters and technological disasters, particularly those caused by human intent. Natural disasters “create a social context marked by an initial overwhelming consensus regarding priorities and the allocation of resources,”<sup>15</sup> which explains the enormous outpouring of voluntary support following the floods of 1993. In contrast to natural disasters, which “occur as purpose-

<sup>14</sup> Norris, et al, “60,000 Disaster Victims Speak: Part II. Summary and Implications of the Disaster Mental Health Research,” *Psychiatry*, Fall 2002, 65, 3, Health Module.

<sup>15</sup> Warheit, G.J., “A note on natural disasters and civil disturbances: Similarities and differences.” *Mass Emergencies*, 1, 1976, pp. 131-137.

less, asocial events; civil disturbances can be viewed as instrumentally initiated to achieve certain social goals.”<sup>16</sup> An EMP attack would certainly be perceived similarly, whether the adversary were a terrorist organization or a state.

The selected case studies provide only an approximation of EMP effects. For example, the effects of the knowledge that widespread infrastructure disruption resulted from an intentional foreign attack are yet unknown. Much evidence points to people’s resilience in the immediate aftermath of disasters. However, during a lengthy recovery process, as would be expected following an EMP attack with widespread, long-duration effects, the psychological effects of the attack should not be underestimated.

It appears clear that the most crucial question in the task of avoiding social disorder is how to establish communication without electricity immediately following an EMP attack. Without communication alternatives, it would be impossible to alert people to the availability of emergency supplies or inform them concerning emergency response activities. It also appears clear that greater awareness of the nature of an EMP attack and knowledge of what prudent preparations might be undertaken to mitigate its consequences would be desirable. Accordingly we make the following recommendations.

### Recommendations

- ◆ Support to national leadership should involve measures to ensure that the President can communicate effectively with the citizenry.
- ◆ Because many citizens would be without power, communications, and other services for days — or perhaps substantially longer — before full recovery could occur, during that interval, it will be crucial to provide a reliable channel of information to citizens to let them know what has happened, what the current situation is, when help of what types might be available, what their governments are doing, and answers to the host of other questions that, if not answered, would almost certainly create more instability and suffering for the affected individuals, communities, and the Nation as a whole. In particular:
  - The Department of Homeland Security should play a leading role in spreading knowledge of the nature of prudent mitigation preparations for EMP attack to mitigate its consequences.
  - The Department of Homeland Security should add content to Web sites it maintains, such as [www.Ready.gov](http://www.Ready.gov), which provides concise overviews of the threats posed by EMP attacks and geomagnetic storms, summarizes steps that people should take given an incident and identifies alternate or emergency communications channels.
  - The Department of Homeland Security should work with state homeland security organizations to develop and exercise communications networks involving the organizations that normally operate in each community.

---

<sup>16</sup> Ibid.

## Appendix A. The Commission and Its Charter

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack was established by Congress through Title XIV of Public Law 106-398. Looking out 15 years, the Commission was tasked to assess:

- 1) The nature and magnitude of potential high-altitude EMP threats to the United States from all potentially hostile states or non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to perform a high-altitude EMP attack against the United States within the next 15 years.
- 2) The vulnerability of United States military and especially civilian systems to an EMP attack, giving special attention to vulnerability of the civilian infrastructure as a matter of emergency preparedness.
- 3) The capability of the United States to repair and recover from damage inflicted on United States military and civilian systems by an EMP attack.
- 4) The feasibility and cost of hardening select military and civilian systems against EMP attack.

The Commission was also tasked to recommend any steps it believes should be taken by the United States to better protect its military and civilian systems from EMP attack.

In accord with its charter, the Commission focused on the electromagnetic pulse produced by high-altitude nuclear weapon detonations, as opposed to other types of nuclear and non-nuclear EMP phenomena. Unless clearly indicated to the contrary, all references to EMP are to the electromagnetic pulse produced by a high-altitude nuclear detonation.

This report presents the unanimous conclusions and recommendations of the Commissioners.

### Organization

Commissioners were nominated by the Secretary of Defense and by the Administrator of the Federal Emergency Management Agency<sup>1</sup>:

- ◆ Dr. William R. Graham (Chairman)
- ◆ Dr. John S. Foster, Jr.
- ◆ Mr. Earl Gjelde
- ◆ Dr. Robert J. Hermann
- ◆ Mr. Henry (Hank) M. Kluepfel
- ◆ Gen Richard L. Lawson, USAF (Ret.)
- ◆ Dr. Gordon K. Soper
- ◆ Dr. Lowell J. Wood, Jr.
- ◆ Dr. Joan B. Woodard

Commissioners brought to this task a wide range of expertise, including service as an advisor to the President; senior management experience in both civilian and military agencies, National Laboratories, and the corporate sector; management and operation of national infrastructures, and technical expertise in the design of nuclear weapons and in the hardening of systems against nuclear weapon effects. Commissioner resumes are provided in an appendix to this volume.

---

<sup>1</sup> The Federal Emergency Management Agency was an independent agency when the Commission was established; it is now a component within the Department of Homeland Security.

Dr. Michael J. Frankel served as Executive Director of the Commission. He was also responsible for overseeing the technical efforts in support of the Commission accomplished by both American and foreign organizations. The Institute for Defense Analysis, under the leadership of Dr. Rob Mahoney, provided staff and facilities support for the Commission. Dr. Peter Pry provided liaison with the Congress. The Commission also benefited from the understanding of EMP available in foreign institutions. Several government, non-profit, and commercial organizations conducted work and prepared reports for the Commission.

## Method

The Commission employed a capabilities-based methodology to assess potential high-altitude EMP threats to the United States over the next 15 years.<sup>2</sup> To this end it engaged the current Intelligence Community, sponsored the acquisition of new test data and performed analytic studies as input to the independent assessment developed by the Commission. Fifteen years is a very long time horizon. Many developments are possible, to include actions by the United States and others that can shape this future in a variety of ways. At the Commission's inception, Iraq was a state of concern from the standpoint of nuclear proliferation and potential EMP threats. Due to actions taken by the Coalition, such Iraqi capabilities are no longer a current concern.

...a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered looks strange; what looks strange is therefore improbable; what seems improbable need not be considered seriously.

— Thomas C. Schelling, in Roberta Wohlstetter, *Pearl Harbor: Warning and Decision*. Stanford University Press, 1962, p. vii

The Commission did not attempt to forecast the relative likelihood of alternative WMD threat scenarios. Instead, it sponsored research and reviewed existing assessments to identify the capabilities that might be available to adversaries, with particular emphasis on ballistic missile and nuclear weapons needed for EMP attacks.

The Commission's charter encompassed all types of high-altitude EMP threats. The Commission made a decision to focus most of its efforts on the most feasible of these threats – EMP attacks involving one or a few weapons that could cause serious damage to the functioning of the United States as a society or result in undermining national support to American forces during a regional contingency.

## Activities

The Commission received excellent support from the Intelligence Community, particularly the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, and Department of Energy Office of Intelligence. National Nuclear Security Administration laboratories (Lawrence Livermore, Los Alamos, and Sandia), the Navy, and the Defense Threat Reduction Agency provided excellent technical support to the Commission's analyses. While it benefited from these inputs, the Commission developed an independent assessment, and is solely responsible for the content of its research, conclusions, and recommendations in this report.

<sup>2</sup> This methodology is addressed in a Commission staff paper — Rob Mahoney, *Capabilities-Based Methodology for Assessing Potential Adversary Capabilities*, March 2004.

The Commission also reviewed relevant foreign research and programs, and assessed foreign perspectives on EMP attacks.

In considering EMP, the Commission also gave attention to the coincident nuclear effects that would result from a high-altitude detonation that produces EMP, e.g., possible disruption of the operations of, or damage to, satellites in a range of orbits around the Earth.

In addition to examining potential threats, the Commission was charged to assess U.S. vulnerabilities (civilian and military) to EMP and to recommend measures to counter EMP threats. For these purposes, the Commission reviewed research and best practices within the United States and other countries.

Early in this review it became apparent that only limited EMP vulnerability testing had been accomplished for modern electronic systems and components. To partially remedy this deficit, the Commission sponsored illustrative testing of current systems and infrastructure components.





## Appendix B. Biographies

*Dr. William R. Graham* is Chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. He is the retired Chairman of the Board and Chief Executive Officer of National Security Research Inc. (NSR), a Washington-based company that conducted technical, operational, and policy research and analysis related to U.S. national security. He currently serves as a member of the Department of Defense's Defense Science Board and the National Academies Board on Army Science and Technology. In the recent past he has served as a member of several high-level study groups, including the Department of Defense Transformation Study Group, the Commission to Assess United States National Security Space Management and Organization, and the Commission to Assess the Ballistic Missile Threat to the United States. From 1986–89 Dr. Graham was the director of the White House Office of Science and Technology Policy, while serving concurrently as Science Advisor to President Reagan, Chairman of the Federal Joint Telecommunications Resources Board, and a member of the President's Arms Control Experts Group.

*Dr. John S. Foster, Jr.*, is Chairman of the Board of GKN Aerospace Transparency Systems, and consultant to Northrop Grumman Corporation, Technology Strategies & Alliances, Sikorsky Aircraft Corp., Intellectual Ventures, Lawrence Livermore National Lab, Ninesigma, and Defense Group. He retired from TRW as Vice President, Science and Technology, in 1988 and continued to serve on the Board of Directors of TRW from 1988 to 1994. Dr. Foster was Director of Defense Research and Engineering for the Department of Defense from 1965–1973, serving under both Democratic and Republican administrations. In other distinguished service, Dr. Foster has been on the Air Force Scientific Advisory Board, the Army Scientific Advisory Panel, and the Ballistic Missile Defense Advisory Committee, Advanced Research Projects Agency. Until 1965, he was a panel consultant to the President's Science Advisory Committee, and from 1973–1990 he was a member of the President's Foreign Intelligence Advisory Board. He is a member of the Defense Science Board, which he chaired from January 1990–June 1993. From 1952–1962, Dr. Foster was with Lawrence Livermore National Laboratory (LLNL), where he began as a Division Leader in experimental physics, became Associate Director in 1958, and became Director of LLNL and Associate Director of the Lawrence Berkeley National Laboratory in 1961.

*Mr. Earl Gjelde* is the President and Chief Executive Officer of Summit Power Group Inc., and several affiliated companies, primary participants in the development of over 5,000 megawatts of natural gas fired electric and wind generating plants within the United States. He has served on the boards of EPRI and the U.S. Energy Association among others. He has held a number of U.S.A. government posts, serving as President George Herbert Walker Bush's Under (now called Deputy) Secretary and Chief Operating Officer of the U.S. Department of the Interior (1989) and serving President Ronald Reagan as Under Secretary and Chief Operating Officer of the U.S. Department of the Interior (1985–1988), the Counselor to the Secretary and Chief Operating Officer of the U.S. Department of Energy (1982–1985); and Deputy Administrator, Power Manager and Chief Operating Officer of the Bonneville Power Administration (1980–1982). While in the Reagan Administration he served concurrently as Special Envoy to China (1987), Deputy Chief of Mission for the U.S.-Japan Science and Technology Treaty (1987–1988), and Counselor for Policy to the Director of the National Critical Materials Council

(1986–1988). Prior to 1980, he was a Principal Officer of the Bonneville Power Administration.

*Dr. Robert J. Hermann* is a Senior Partner of Global Technology Partners, LLC, a consulting firm that focuses on technology, defense aerospace, and related businesses worldwide. In 1998, Dr. Hermann retired from United Technologies Corporation (UTC), where he was Senior Vice President, Science and Technology. Prior to joining UTC in 1982, Dr. Hermann served 20 years with the National Security Agency with assignments in research and development, operations, and NATO. In 1977, he was appointed Principal Deputy Assistant Secretary of Defense for Communications, Command, Control, and Intelligence. In 1979, he was named Assistant Secretary of the Air Force for Research, Development, and Logistics and concurrently was Director of the National Reconnaissance Office.

*Mr. Henry (Hank) M. Kluepfel* is a Vice President for Corporate Development at SAIC. He is the company's leading cyberspace security advisor to the President's National Security Telecommunications Advisory Committee (NSTAC) and the Network Reliability and Interoperability Council (NRIC). Mr. Kluepfel is widely recognized for his 30-plus years of experience in security technology research, design, tools, forensics, risk reduction, education, and awareness, and he is the author of industry's de facto standard security base guideline for the Signaling System Number 7(SS7) networks connecting and controlling the world's public telecommunications networks. In past affiliations with Telcordia Technologies (formerly Bellcore), AT&T, BellSouth and Bell Labs, he led industry efforts to protect, detect, contain, and mitigate electronic and physical intrusions and led the industry's understanding of the need to balance technical, legal, and policy-based countermeasures to the then emerging hacker threat. He is recognized as a Certified Protection Professional by the American Society of Industrial Security and is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

*General Richard L. Lawson, USAF (Ret.)*, is Chairman of Energy, Environment and Security Group, Ltd., and former President and CEO of the National Mining Association. He also serves as Vice Chairman of the Atlantic Council of the U.S.; Chairman of the Energy Policy Committee of the U.S. Energy Association; Chairman of the United States delegation to the World Mining Congress; and Chairman of the International Committee for Coal Research. Active duty positions included serving as Military Assistant to the President; Commander, 8th Air Force; Chief of Staff, Supreme Headquarters Allied Powers Europe; Director for Plans and Policy, Joint Chiefs of Staff; Deputy Director of Operations, Headquarters U.S. Air Force; and Deputy Commander in Chief, U.S. European Command.

*Dr. Gordon K. Soper* is employed by Defense Group Inc. There he has held various senior positions where he was responsible for broad direction of corporate goals relating to company support of government customers in areas of countering the proliferation of weapons of mass destruction, nuclear weapons effects and development of new business areas and growth of technical staff. He provides senior-level technical support on a range of task areas to the Defense Threat Reduction Agency (DTRA) and to a series of Special Programs for the Office of the Secretary of Defense and the White House Military Office. Previously, Dr. Soper was Principal Deputy to the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Programs (ATSD(NCB)); Director, Office of Strategic and Theater Nuclear Forces Command, Control and Communications (C3) of

the Office of the Assistant Secretary of Defense (C3I); Associate Director for Engineering and Technology/Chief Scientist at the Defense Communications Agency (now DISA); and held various leadership positions at the Defense Nuclear Agency (now DTRA).

*Dr. Lowell L. Wood, Jr.*, is a scientist-technologist who has contributed to technical aspects of national defense, especially defense against missile attack, as well as to controlled thermonuclear fusion, laser science and applications, optical and underwater communications, very high-performance computing and digital computer-based physical modeling, ultra-high-power electromagnetic systems, space exploration and climate-stabilization geophysics. Wood obtained his Ph.D. in astrophysics and planetary and space physics at UCLA in 1965, following receipt of bachelor's degrees in chemistry and math in 1962. He has held faculty and professional research staff appointments at the University of California (from which he retired after more than four decades in 2006) and is a Research Fellow at the Hoover Institution at Stanford University. He has advised the U.S. Government in many capacities, and has received a number of awards and honors from both government and professional bodies. Wood is the author, co-author or editor of more than 200 unclassified technical papers and books and more than 300 classified publications, and is named as an inventor on more than 200 patents and patents-pending.

*Dr. Joan B. Woodard* is Executive Vice President and Deputy Laboratories Director for Nuclear Weapons at Sandia National Laboratories. Sandia's role is to provide engineering support and design to the Nation's nuclear weapons stockpile, provide our customers with research, development, and testing services, and manufacture specialized non-nuclear products and components for national defense and security applications. The laboratories enable safe and secure deterrence through science, engineering, and management excellence. Prior to her current assignment, Dr. Woodard served as Executive Vice President and Deputy Director, responsible for Sandia's programs, operations, staff and facilities; developing policy and assuring implementation; and strategic planning. Her Sandia history began in 1974, and she rose through the ranks to become the Director of the Environmental Programs Center and the Director of the Product Realization Weapon Components Center; Vice President of the Energy & Environment Division and Vice President of the Energy Information and Infrastructure Technologies Division. Joan has been elected to the Phi Kappa Phi Honor Society and has served on numerous external panels and boards, including the Air Force Scientific Advisory Board, the National Academy of Sciences' Study on Science and Technology for Countering Terrorism, the Secretary of Energy's Nuclear Energy Research Advisory Council, the Congressional Commission on Electromagnetic Pulse, and the Intelligence Science Board. Joan has received many honors, including the Upward Mobility Award from the Society of Women Engineers, and was named as "One of Twenty Women to Watch in the New Millennium" by the Albuquerque Journal. She also received the Spirit of Achievement Award from National Jewish Hospital.

*Dr. Michael J. Frankel* is Executive Director of the EMP Commission and one of the Nation's leading experts on the effects of nuclear weapons. Formerly he served as Associate Director for Advanced Energetics and Nuclear Weapons, Office of the Deputy Undersecretary of Defense (S&T); Chief Scientist, Nuclear Phenomenology Division, Defense Threat Reduction Agency; Congressional Fellow, U.S. Senate; Chief Scientist, Strategic Defense Initiative Organization Lethality Program; and as a Research Physicist at the Naval Surface Warfare Center, White Oak. In prior government service, Dr.

Frankel directed significant elements of the core national Nuclear Weapons Phenomenology program along with major WMD, Directed Energy, and Space System technology programs at the Defense Nuclear Agency while coordinating activities between the Military Services, National Laboratories, and industrial S&T organizations to address strategic defense technology needs. He has been an active participant in international scientific exchanges in his role as Executive Secretary for the U.S. – United Kingdom Joint Working Group under terms of the 1958 Atomic Treaty, and as Chairman of both the Novel Energetics and Hard Target Defeat working groups under the TTCP agreement with the UK, Australia, Canada and New Zealand. He has also delivered invited lectures, chaired national and international technical symposia, and published numerous articles in the professional scientific literature. He holds a Ph.D. in Theoretical Physics from New York University.





ISBN 978-0-16-080927-9



9 780160 809279

# Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

## *Volume 1: Executive Report* *2004*

Dr. John S. Foster, Jr.

Mr. Earl Gjelde

Dr. William R. Graham (Chairman)

Dr. Robert J. Hermann

Mr. Henry (Hank) M. Kluepfel

GEN Richard L. Lawson, USAF (Ret.)

Dr. Gordon K. Soper

Dr. Lowell L. Wood, Jr.

Dr. Joan B. Woodard



## CHARTER

Public Law 106-398, Title XIV

### SEC. 1402. DUTIES OF COMMISSION

(a) Review of EMP Threat. The Commission shall assess:

(1) the nature and magnitude of potential high-altitude EMP threats to the United States from all potentially hostile states or non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to perform a high-altitude EMP attack against the United States within the next 15 years;

(2) the vulnerability of United States military and especially civilian systems to an EMP attack, giving special attention to vulnerability of the civilian infrastructure as a matter of emergency preparedness;

(3) the capability of the United States to repair and recover from damage inflicted on United States military and civilian systems by an EMP attack; and

(4) the feasibility and cost of hardening select military and civilian systems against EMP attack.

(b) Recommendation. The Commission shall recommend any steps it believes should be taken by the United States to better protect its military and civilian systems from EMP attack.

The findings and recommendations presented in this report are the independent judgments of this Commission and should not be attributed to any other people or organizations. This report presents the unanimous views of the Commissioners.





## ABSTRACT

Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse (EMP). A determined adversary can achieve an EMP attack capability without having a high level of sophistication.

EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences. EMP will cover the wide geographic region within line of sight to the nuclear weapon. It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of US society, as well as to the ability of the United States and Western nations to project influence and military power.

The common element that can produce such an impact from EMP is primarily electronics, so pervasive in all aspects of our society and military, coupled through critical infrastructures. Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow. The impact of EMP is asymmetric in relation to potential protagonists who are not as dependent on modern electronics.

The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected. Correction is feasible and well within the Nation's means and resources to accomplish.



# CONTENTS

OVERVIEW: EMP IS CAPABLE OF CAUSING CATASTROPHE FOR THE NATION.....	1
WE CAN PREVENT AN EMP CATASTROPHE.....	4
Nature of the EMP Threat.....	4
Prevention .....	7
Protection and Recovery of Civilian Infrastructures .....	8
STRATEGY AND RECOMMENDATIONS .....	11
Intelligence, Interdiction, and Deterrence.....	11
Protecting Critical Components of the Infrastructure.....	12
Maintaining the Capability to Monitor and Evaluate the Condition of Critical Infrastructures.....	12
Recognizing EMP Attack .....	12
Planning to Carry Out a Systematic Recovery of Critical Infrastructures.....	14
Training, Evaluating, Red Teaming, and Periodically Reporting to the Congress.....	14
Defining the Federal Government’s Responsibility and Authority to Act .....	15
Recognizing the Opportunities for Shared Benefits .....	16
Conducting Research and Development.....	16
ELECTRIC POWER INFRASTRUCTURE .....	17
Nature of the Problem.....	17
Recommended Mitigation and Responsibility.....	19
Protection .....	20
Restoration .....	20
Essential Component Protection .....	21
System Restoration .....	22
TELECOMMUNICATIONS .....	24
Importance of Assured Telecommunications .....	24
EMP Effects on Telecommunications .....	28
Recommended Mitigation Activities .....	28

BANKING AND FINANCE.....	31
Nature of the Problem.....	31
Recommended Mitigation and Responsibility.....	33
FUEL/ENERGY INFRASTRUCTURE.....	35
TRANSPORTATION INFRASTRUCTURE.....	36
Nature of the Problem.....	36
Strategy for Protection and Recovery.....	37
FOOD INFRASTRUCTURE .....	40
Nature of the Problem.....	40
Mitigation and Responsibility.....	40
WATER SUPPLY INFRASTRUCTURE .....	42
EMERGENCY SERVICES .....	43
Vulnerabilities.....	43
Recommended Strategy for Protection and Recovery.....	43
SPACE SYSTEMS.....	44
GOVERNMENT.....	45
KEEPING THE CITIZENRY INFORMED.....	46
PROTECTION OF MILITARY FORCES .....	47

## APPENDIXES

A The Commission and Its Method.....	A-1
B Commissioners.....	B-1

## FIGURES

1 Starfish Nuclear Detonation.....	5
2 Illustrative EMP Effects – Fast Pulse .....	6
3 Illustrative EMP Effects – Slow Pulse Protection and Recovery of Civilian Infrastructures .....	7
4 Interdependent Infrastructure Sectors.....	9
5 Extent of 1989 Geomagnetic Storm.....	17



## OVERVIEW

### EMP IS CAPABLE OF CAUSING CATASTROPHE FOR THE NATION

The high-altitude nuclear weapon-generated electromagnetic pulse (EMP) is one of a small number of threats that has the potential to hold our society seriously at risk and might result in defeat of our military forces.

Briefly, a single nuclear weapon exploded at high altitude above the United States will interact with the Earth's atmosphere, ionosphere, and magnetic field to produce an electromagnetic pulse (EMP) radiating down to the Earth and additionally create electrical currents in the Earth. EMP effects are both direct and indirect. The former are due to electromagnetic "shocking" of electronics and stressing of electrical systems, and the latter arise from the damage that "shocked"—upset, damaged, and destroyed—electronics controls then inflict on the systems in which they are embedded.

*The damage level could be sufficient to be catastrophic to the Nation, and our current vulnerability invites attack.*

The indirect effects can be even more severe than the direct effects.

The electromagnetic fields produced by weapons designed and deployed with the intent to produce EMP have a high likelihood of damaging electrical power systems, electronics, and information systems upon which American society depends. Their effects on dependent systems and infrastructures could be sufficient to qualify as catastrophic to the Nation.

Depending on the specific characteristics of the attacks, unprecedented cascading failures of our major infrastructures could result. In that event, a regional or national recovery would be long and difficult and would seriously degrade the safety and overall viability of our Nation. The primary avenues for catastrophic damage to the Nation are through our electric power infrastructure and thence into our telecommunications, energy, and other infrastructures. These, in turn, can seriously impact other important aspects of our Nation's life, including the financial system; means of getting food, water, and medical care to the citizenry; trade; and production of goods and services. The recovery of any one of the key national infrastructures is dependent on the recovery of others. The longer the outage, the more problematic and uncertain the recovery will be. It is possible

for the functional outages to become mutually reinforcing until at some point the degradation of infrastructure could have irreversible effects on the country's ability to support its population.

EMP effects from nuclear bursts are not new threats to our nation. The Soviet Union in the past and Russia and other nations today are potentially capable of creating these effects. Historically, this application of nuclear weaponry was mixed with a much larger population of nuclear devices that were the primary source of destruction, and thus EMP as a weapons effect was not the primary focus. Throughout the Cold War, the United States did not try to protect its civilian infrastructure against either the physical or EMP impact of nuclear weapons, and instead depended on deterrence for its safety.

What is different now is that some potential sources of EMP threats are difficult to deter—they can be terrorist groups that have no state identity, have only one or a few weapons, and are motivated to attack the US without regard for their own safety. Rogue states, such as North Korea and Iran, may also be developing the capability to pose an EMP threat to the United States, and may also be unpredictable and difficult to deter.

Certain types of relatively low-yield nuclear weapons can be employed to generate potentially catastrophic EMP effects over wide geographic areas, and designs for variants of such weapons may have been illicitly trafficked for a quarter-century.

China and Russia have considered limited nuclear attack options that, unlike their Cold War plans, employ EMP as the primary or sole means of attack. Indeed, as recently as May 1999, during the NATO bombing of the former Yugoslavia, high-ranking members of the Russian Duma, meeting with a US congressional delegation to discuss the Balkans conflict, raised the specter of a Russian EMP attack that would paralyze the United States.

Another key difference from the past is that the US has developed more than most other nations as a modern society heavily dependent on electronics, telecommunications, energy, information networks, and a rich set of financial and transportation systems that leverage modern technology. This asymmetry is a source of substantial economic, industrial, and societal advantages, but it creates vulnerabilities and critical interdependencies that are potentially disastrous to the United States. Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack. The current vulnerability of US

critical infrastructures can both invite and reward attack if not corrected; however, correction is feasible and well within the Nation's means and resources to accomplish.

## WE CAN PREVENT AN EMP CATASTROPHE

The Nation's vulnerability to EMP that gives rise to potentially large-scale, long-term consequences can be reasonably and readily reduced below the level of a potentially catastrophic national problem by coordinated and focused effort between the private and public sectors of our country. The cost for such improved security in the next 3 to 5 years is modest by any standard—and extremely so in relation to both the war on terror and the value of the national infrastructures involved. The appropriate response to this threatening situation is a balance of prevention, protection, planning, and preparations for recovery. Such actions are both rational and feasible. A number of these actions also reduce vulnerabilities to other serious threats to our infrastructures, thus giving multiple benefits.

### NATURE OF THE EMP THREAT

High-altitude EMP results from the detonation of a nuclear warhead at altitudes of about 40 to 400 kilometers above the Earth's surface. The immediate effects of EMP are disruption of, and damage to, electronic systems and electrical infrastructure. EMP is not reported in the scientific literature to have direct effects on people in the parameter range of present interest.

EMP and its effects were observed during the US and Soviet atmospheric test programs in 1962. Figure 1 depicts the Starfish nuclear detonation—not designed or intended as a generator of EMP—at an altitude of about 400 kilometers above Johnston Island in the Pacific Ocean. Some electronic and electrical systems in the Hawaiian Islands, 1400 kilometers distant, were affected, causing the failure of street-lighting systems, tripping of circuit breakers, triggering of burglar alarms, and damage to a telecommunications relay facility. In their testing that year, the Soviets executed a series of nuclear detonations in which they exploded 300 kiloton weapons at approximately 300, 150, and 60 kilometers above their test site in South Central Asia. They report that on each shot they observed damage to overhead and underground buried cables at distances of 600 kilometers. They also observed surge arrestor burnout, spark-gap breakdown, blown fuses, and power supply breakdowns.

What is significant about an EMP attack is that one or a few high-altitude nuclear detonations can produce EMP effects that can potentially disrupt or damage electronic

and electrical systems over much of the United States, virtually simultaneously, at a time determined by an adversary.



Widespread red air glow (6300 Å) amid dark clouds, caused mostly by x-ray-excited atomic oxygen (i.e., oxygen by photoelectrons liberated by Starfish X-rays)

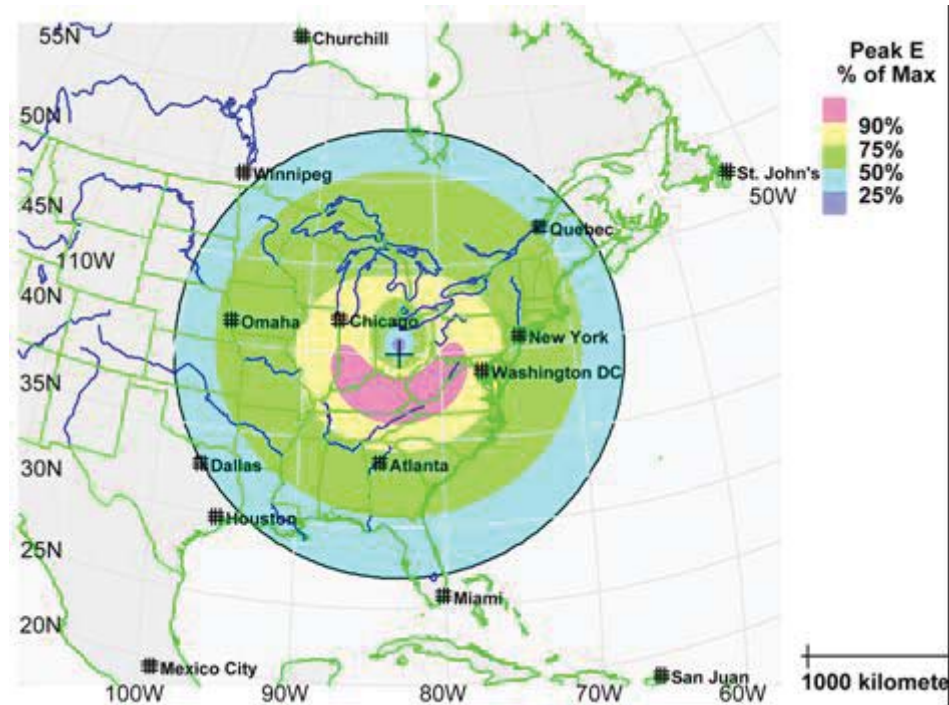
### **Figure 1. Starfish Nuclear Detonation**

Gamma rays from a high-altitude nuclear detonation interact with the atmosphere to produce a radio-frequency wave of unique, spatially varying intensity that covers everything within line-of-sight of the explosion's center point. It is useful to focus on three major EMP components.

#### *FIRST EMP COMPONENT (E1)*

The first component is a free-field energy pulse with a rise-time measured in the range of a fraction of a billionth to a few billionths of a second. It is the "electromagnetic shock" that disrupts or damages electronics-based control systems, sensors, communication systems, protective systems, computers, and similar devices. Its damage or functional disruption occurs essentially simultaneously over a very large area, as illustrated in Figure 2.





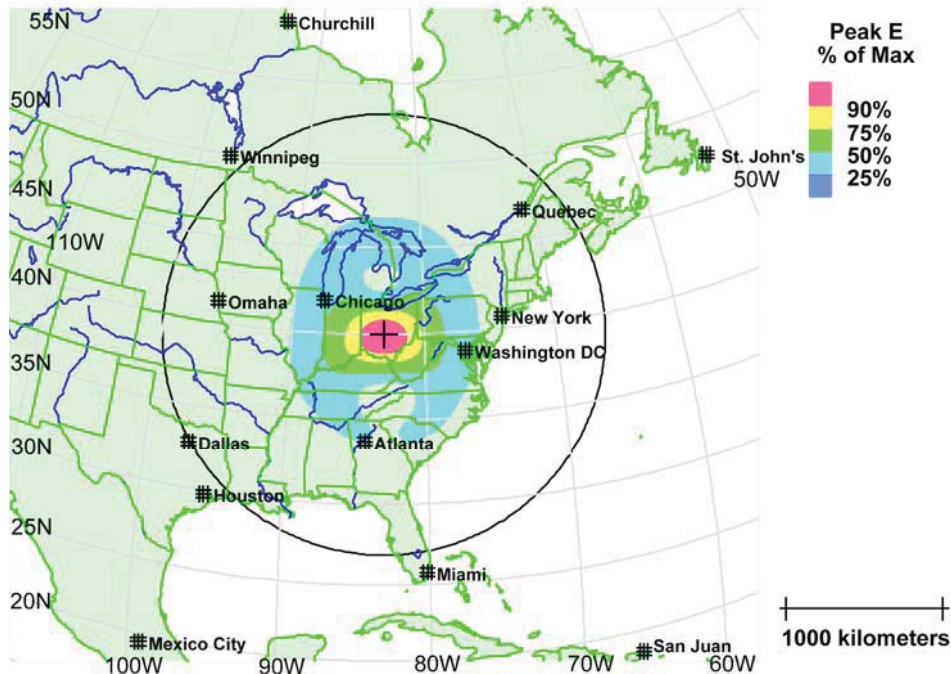
**Figure 2. Illustrative EMP Effects – Fast Pulse**

#### *SECOND EMP COMPONENT (E2)*

The middle-time component covers roughly the same geographic area as the first component and is similar to lightning in its time-dependence, but is far more geographically widespread in its character and somewhat lower in amplitude. In general, it would not be an issue for critical infrastructure systems since they have existing protective measures for defense against occasional lightning strikes. The most significant risk is synergistic, because the E2 component follows a small fraction of a second after the first component's insult, which has the ability to impair or destroy many protective and control features. The energy associated with the second component thus may be allowed to pass into and damage systems.

#### *THIRD EMP COMPONENT (E3)*

The final major component of EMP is a subsequent, slower-rising, longer-duration pulse that creates disruptive currents in long electricity transmission lines, resulting in damage to electrical supply and distribution systems connected to such lines (Figure 3). The sequence of E1, E2, and then E3 components of EMP is important because each can cause damage, and the later damage can be increased as a result of the earlier damage. In the example depicted in Figures 2 and 3, about 70% of the total electrical power load of the United States is within the region exposed to the EMP event.



**Figure 3. Illustrative EMP Effects – Slow Pulse Protection and Recovery of Civilian Infrastructures**

#### PREVENTION

An EMP attack is one way for a terrorist activity to use a small amount of nuclear weaponry—potentially just one weapon—in an effort to produce a catastrophic impact on our society, but it is not the only way. In addition, there are potential applications of surface-burst nuclear weaponry, biological and chemical warfare agents, and cyber attacks that might cause damage that could reach large-scale, long-term levels. The first order of business is to prevent any of these attacks from occurring.

The US must establish a global environment that will profoundly discourage such attacks. We must persuade nations to forgo obtaining nuclear weapons or to provide acceptable assurance that these weapons will neither threaten the vital interests of the United States nor fall into threatening hands.

For all others, we must make it difficult and dangerous to acquire the materials to make a nuclear weapon and the means to deliver them. We must hold at risk of capture or destruction anyone who has such weaponry, wherever they are in the world.

*The first order of business is to prevent any of these attacks from occurring.*

Those who engage in or support these activities must be made to understand that they do so at the risk of everything they value. Those who harbor or help those who conspire to create these weapons must suffer serious consequences as well.

In case these measures do not completely succeed, we must have vigorous interdiction and interception efforts to thwart delivery of all such weaponry. To support this strategy, the US must have intelligence capabilities sufficient to understand what is happening at each stage of developing threats. In summary, the costs of mounting such attacks must be made to be great in all respects, and the likelihood of successful attack rendered unattractively small.

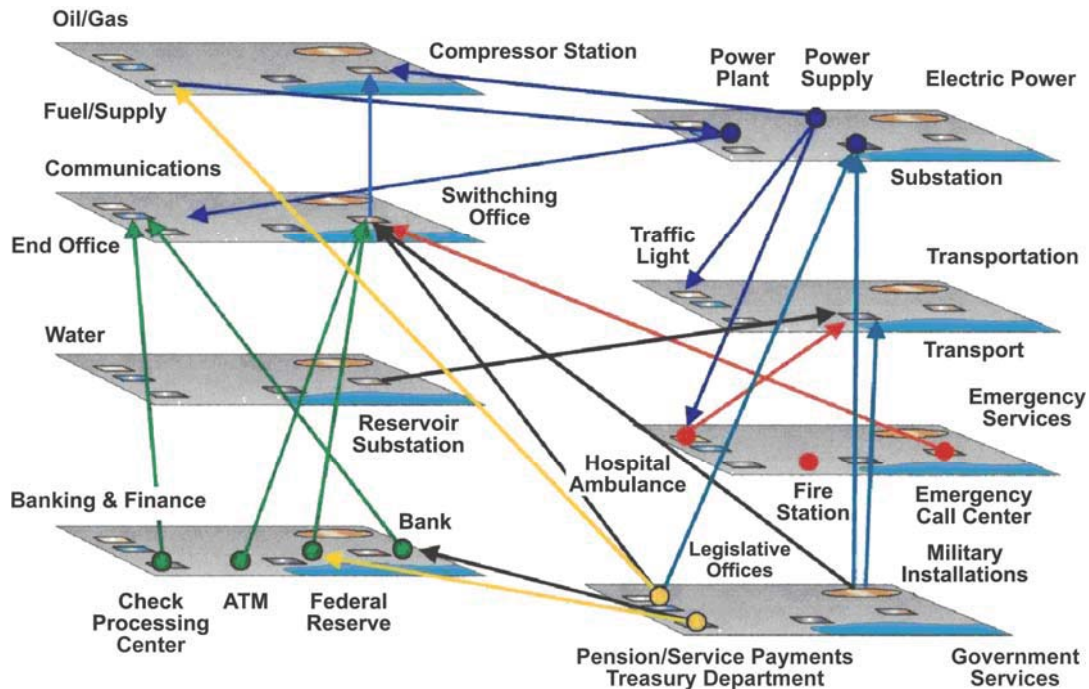
The current national strategy for war on terrorism already contains all of these elements. The threat of an EMP attack further raises what may be at stake.

To further forestall an EMP attack, we must reduce our vulnerability to EMP and develop our ability to recover, should there be an attack, in order to reduce the incentives to use such weaponry. We should never allow terrorists or rogue states a “cheap shot” that has such a large and potentially devastating impact.

#### PROTECTION AND RECOVERY OF CIVILIAN INFRASTRUCTURES

Each critical infrastructure in the US is dependent upon other infrastructures (Figure 4). The interdependence on the proper functioning of such systems constitutes a hazard when threat of widespread failures exists. The strong interdependence of our critical national infrastructures may cause unprecedented challenges in attempts to recover from the widespread disruption and damage that would be caused by an EMP attack.

All of the critical functions of US society and related infrastructures—electric power, telecommunications, energy, financial, transportation, emergency services, water, food, etc.—have electronic devices embedded in most aspects of their systems, often providing critical controls. Electric power has thus emerged as an essential service underlying US society and all of its other critical infrastructures. Telecommunications has grown to a critical level but may not rise to the same level as electrical power in terms of risk to the Nation’s survival. All other infrastructures and critical functions are dependent upon the support of electric power and telecommunications. Therefore, we must make special efforts to prepare and protect these two high-leverage systems.



**Figure 4. Interdependent Infrastructure Sectors**

Most critical infrastructure system vulnerabilities can be reduced below the level that potentially invites attempts to create a national catastrophe. By protecting key elements in each critical infrastructure and by preparing to recover essential services, the prospects for a terrorist or rogue state being able to achieve large-scale, long-term damage can be minimized. This can be accomplished reasonably and expeditiously.

Such preparation and protection can be achieved over the next few years, given a dedicated commitment by the federal government and an affordable investment of resources. We need to take actions and allocate resources to decrease the likelihood that catastrophic consequences from an EMP attack will occur, to reduce our current serious level of vulnerability to acceptable levels and thereby reduce incentives to attack, and to remain a viable modern society even if an EMP attack occurs. Since this is a matter of national security, the federal government must shoulder the responsibility of managing the most serious infrastructure vulnerabilities.

*The most critical infrastructure system vulnerabilities can be reduced below those levels that invite attack or cause a national catastrophe.*

Homeland Security Presidential Directives 7 and 8 lay the authoritative basis for the Federal government to act vigorously and coherently to mitigate many of the risks to the Nation from terrorist attack. The effects of EMP on our major infrastructures lie

within these directives, and the directives specify adequate responsibilities and provide sufficient authorities to deal with the civilian sector consequences of an EMP attack.

In particular, the Department of Homeland Security (DHS) has been established, led by a Secretary with authority, responsibility, and the obligation to request needed resources for the mission of protecting the US and recovering from the impacts of the most serious threats. This official must assure that plans, resources, and implementing structures are in place to accomplish these objectives, specifically with respect to the EMP threat. In doing so, DHS must work in conjunction with the other established governmental institutions and with experts in the private sector to most efficiently accomplish this mission. It is important that metrics for assessing improvements in prevention, protection, and recovery be put in place and then evaluated and that progress be reported regularly. DHS must clearly and expeditiously delineate its responsibility and actions in relation to other governmental institutions and the private sector, in order to provide clear accountability and avoid confusion and duplication of effort.

Specific recommendations are provided below with respect to both the particulars for securing each of the most critical national infrastructures against EMP threats and the governing principles for addressing these issues of national survival and recovery in the aftermath of EMP attack.



## STRATEGY AND RECOMMENDATIONS

It will not be possible to reduce the incentives for an EMP attack to an acceptable level of risk through defensive protection measures alone. It is possible to achieve an acceptable level of risk and reduced invitation to an EMP attack with a strategy of:

- Pursuing intelligence, interdiction, and deterrence to discourage EMP attack against the US and its interests
- Protecting critical components of the infrastructure, with particular emphasis on those that, if damaged, would require long periods of time to repair or replace
- Maintaining the capability to monitor and evaluate the condition of critical infrastructures
- Recognizing an EMP attack and understanding how its effects differ from other forms of infrastructure disruption and damage
- Planning to carry out a systematic recovery of critical infrastructures
- Training, evaluating, “Red Teaming,” and periodically reporting to the Congress
- Defining the Federal Government’s responsibility and authority to act
- Recognizing the opportunities for shared benefits
- Conducting research to better understand infrastructure system effects and developing cost-effective solutions to manage these effects

The cost for such improved security in the next 3 to 5 years is modest by any standard—and extremely so in relation to both the war on terror and the value of the national infrastructures involved. Costs at later times may be adjusted to deal with the then-apparent threat and future levels of effort required.

### INTELLIGENCE, INTERDICTION, AND DETERRENCE

The federal government’s efforts to establish and maintain a global environment that profoundly discourages potentially catastrophic attacks is our first line of defense. The development, trading, and movement of critical materials and weapons useful for mounting WMD attacks, including those that are based on the use of EMP, must be identified as early in the process as possible. The methods and materials that could encourage an EMP attack must be added to the list of threats presently being sought out and annihilated. The US and its allies against transnational terrorism must make it

exceedingly difficult and dangerous for organizations to position themselves to be a threat, or allow others to use their country and its assets in order to become a threat, specifically including EMP threats. We must hold potential perpetrators at risk of capture or destruction, whenever and wherever in the world they operate.

#### PROTECTING CRITICAL COMPONENTS OF THE INFRASTRUCTURE

Some components of critical infrastructures, such as large turbines, generators, and high-voltage transformers in electrical power systems, and electronic switching systems in telecommunication systems, would require long periods of time to repair or replace. These components should be configured so that even under electronic disruption and damage, such as could be produced by EMP, they do not become further damaged in the course of shutting down or attempting to restore themselves. This type of damage has occurred in the past. During the Northeast power blackout of 1965, Consolidated Edison generators, transformers, motors, and auxiliary equipment were damaged by the sudden shutdown. In particular, the #3 unit at the Ravenswood power plant in New York City suffered damage when the blackout caused loss of oil pressure to the main turbine bearing. The damage kept that unit out of service for nearly a year, and more immediately, complicated and delayed the restoration of service to New York City.

#### MAINTAINING THE CAPABILITY TO MONITOR AND EVALUATE THE CONDITION OF CRITICAL INFRASTRUCTURES

After an EMP attack, system operators and others in positions of authority and responsibility must have immediate access to information sufficient to characterize the state of their critical infrastructure systems. Without such system monitoring and reporting information, the system operators will not have the information required to evaluate the extent of the loss of infrastructure and know how to begin restoration of their systems. They may even induce further damage by taking inappropriate actions or failing to take necessary actions. During the time leading up to the August 14, 2003, Midwest power blackout that affected both the United States and Canada, key system operators did not have a functioning alarm system, did not recognize that the alarm system was not functioning, and had only fragmentary information on the changing configuration of the rapidly collapsing power grid for which they were responsible.

#### RECOGNIZING EMP ATTACK

Electronic upsets and failures occur under normal operating circumstances, even in high-reliability equipment such as that supporting critical infrastructure. EMP-induced

upsets and failures, however, are different from those encountered in the normal operation of infrastructure systems, and in fact have unique aspects not encountered under any other circumstances.

EMP produces nearly simultaneous upset and damage of electronic and of other electrical equipment over wide geographic areas, determined by the altitude, character, and explosive yield of the EMP-producing nuclear explosion. Since such upset and damage is not encountered in other circumstances and particularly not remotely to the same scale, the normal experience of otherwise skilled system operators and others in positions of responsibility and authority will not have prepared them to identify what has happened to the system, what actions to take to minimize further adverse consequences, and what actions must be carried out to restore the impacted systems as swiftly and effectively as possible.

Special system capabilities and operator awareness, planning, training, and testing will be required to deal with EMP-induced system impacts. The first requirement is for the operators of critical infrastructure systems to be able to determine that a high-altitude nuclear explosion has occurred and has produced a unique set of adverse effects on their systems. That information can be provided by local electromagnetic sensors, by information from Earth satellite systems, or by other means. Whatever the means, the operators and others in positions of authority and responsibility must receive the information immediately. Therefore, the EMP event notification system must itself be highly reliable during and after an EMP attack.

Operators and others in positions of authority and responsibility must be trained to recognize that an EMP attack in fact has taken place, to understand the wide range of effects it can produce, to analyze the status of their infrastructure systems, to avoid further system degradation, to dispatch resources to begin effective system restoration, and to sustain the most critical functions while the system is being repaired and restored. Failures similar to those induced by EMP do not occur in normal system operation; therefore, the training for, and experience developed in the course of, normal system operation will not provide operators with the skills and knowledge base necessary to perform effectively after EMP-induced system disruption and failure. Training, procedures, simulations, and exercises must be developed and carried out that are specifically designed to contend with EMP-induced effects.

## PLANNING TO CARRY OUT A SYSTEMATIC RECOVERY OF CRITICAL INFRASTRUCTURES

A crisis such as the immediate aftermath of an EMP attack is not the time to begin planning for an effective response. Plans to avoid causing further damage to critical infrastructures and to carry out a systematic recovery of those infrastructures must be in hand at the earliest possible time. Planning for responding to an EMP attack should begin now and should be carried out jointly by system operators, hardware and software providers, and experts in both the government and private sectors.

Individual infrastructure systems have many similar electronically based control and monitoring functions. The primary features of EMP attack mitigation in each infrastructure include elements of protection of critical functions, identifying where damage within the system is located, dispatch/allocation of resources to allow for timely restoration and development of operational procedures including simulation of both individual and interacting infrastructures, training, testing, and governance. This requires test and evaluation of both existing and future systems to identify weak spots subject to EMP damage and focus mitigation activities accordingly. EMP protection thus has a substantial aspect focused on individual functioning units within each system that contains electronic components, although not necessarily on the individual electronic subcomponents of these units themselves. These units include distributed Supervisory Control and Data Acquisition (SCADA) modules, mobile communicators, radios, embedded control computers, etc. New units can be EMP-hardened for a very small fraction of the cost of the non-hardened item, e.g., 1% to 3% of cost, if hardening is done at the time the unit is designed and manufactured. In contrast, retrofitting existing functional components is potentially an order of magnitude more expensive and should be done only for critical system units. It is important to note, however, that for protection to remain functional, it must be tested and maintained in its operational mode with rigor and discipline.

## TRAINING, EVALUATING, RED TEAMING, AND PERIODICALLY REPORTING TO THE CONGRESS

Identifying an EMP attack, understanding the state of the system after attack, developing and implementing plans for system restoration, and having operators and others in positions of authority and responsibility trained to recognize and respond effectively are elements of strategy that are common to managing the effects of EMP for each of the Nation's critical infrastructure components. Conducting and evaluating the results of training, simulations, tests, and Red Team activities, and periodically reporting

the results to senior executive branch leaders, the Congress, and the public are important elements of being well-prepared for EMP attack, which in turn will sharply reduce the incentives for conduct of such an attack.

#### DEFINING THE FEDERAL GOVERNMENT’S RESPONSIBILITY AND AUTHORITY TO ACT

Governance of the critical infrastructures such as electrical power systems and communications is presently distributed among statutory governmental entities at the federal, state, regional, and municipal levels, as well as among a variety of non-governmental entities. A multiplicity of statutory bodies, private companies, associations, and individual owners also participate in determining decisions and actions. Nevertheless, the process is coordinated, albeit loosely, to produce normal efficient, reliable, and high quality service that is the envy of the world—in a peacetime environment.

A terrorist threat—let alone a terrorist attack—is outside the ambit of normal governance of the key national infrastructures. In dealing with such threats, the Department of Homeland Security has the unique and sole responsibility and authority to govern the specific actions and involved parties within the US, including requesting enabling Congressional funding as appropriate and necessary. DHS must interact with other governmental institutions and the private sector in defining liability, responsibility and funding in order to enable private and government facilities, such as independent power plants, to contribute their capability in a time of national need, yet not interfere with market creation and operation to the maximum extent practical.

***DHS must interact with other governmental institutions and the private sector in defining liability, responsibility, and funding in order to enable private and government facilities, such as independent power plants, to contribute their capability in a time of national need, yet not interfere with market creation and operation to the maximum extent practical.***

Industry associations, system owners/providers, private consultants, and universities all will be able to contribute useful levels of knowledge and skills. DHS is responsible for making the prudent trade-offs within each mitigation activity between performance, risk, schedule, and cost in relation to consequent system protection and then-expected risk in order to achieve maximum protection. For example, some actions taken to protect a system from an EMP attack may diminish the reliability or quality of that system’s normal commercial performance, while other actions may improve the performance.



As an example of resources readily available to DHS with respect to the electric system, the North American Reliability Counsel (NERC) and the Electric Power Research Institute are well-positioned to provide much of the support needed in regard to the EMP threat. Working closely with industry and these institutions, the DHS should provide for the necessary capability to control the national bulk electricity supply system in order to protect critical services, minimize its self-destruction in the event of an EMP attack, and recover its normal capabilities as rapidly and effectively as possible thereafter.

#### RECOGNIZING THE OPPORTUNITIES FOR SHARED BENEFITS

Most of the following initiatives and actions the Commission recommends militate against more than an EMP attack. The protection and/or rapid restoration of critical infrastructures in the civilian sector from an EMP attack also will be effective against other types of infrastructure disruptions, such as attacks aimed at directly damaging or destroying key components of the electrical system, and natural or accidental large-scale disruptions are also significantly mitigated by these same initiatives. Some of these steps also enhance reliability and quality of critical infrastructures, which is a major direct benefit to the US economy and to our way of life.

#### CONDUCTING RESEARCH AND DEVELOPMENT

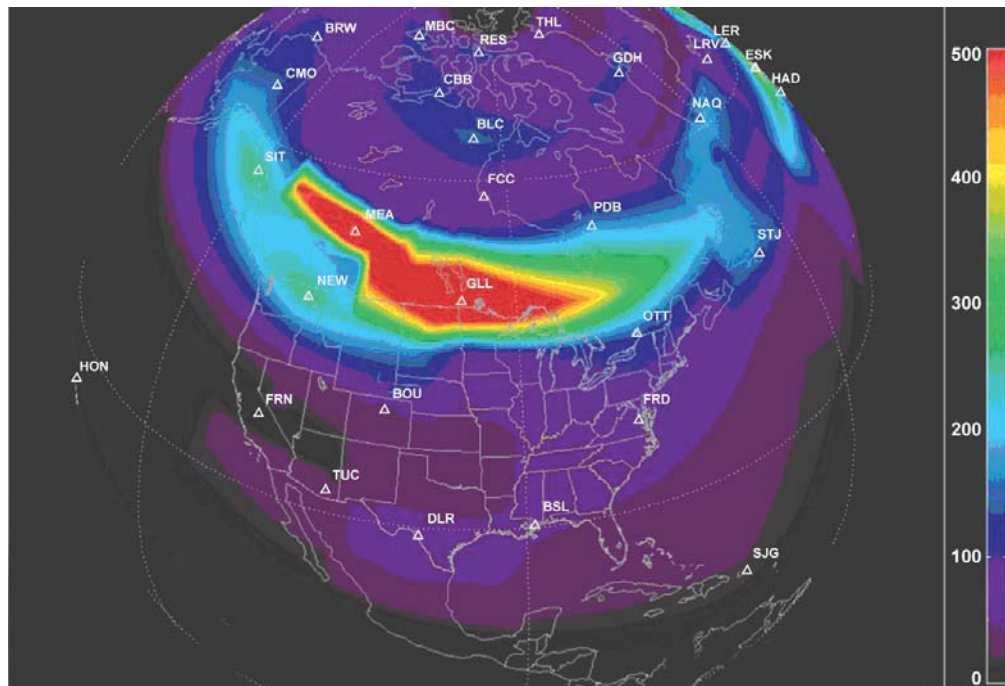
Very little research and development addressing EMP-related system response protection and recovery issues has been done for more than a decade. Conducting research to better understand infrastructure system effects and developing cost-effective solutions to manage these effects will be important to understanding the implications of the rapid evolution of electronics and electrical systems, and their growing role in controlling and operating modern critical infrastructure.

## ELECTRIC POWER INFRASTRUCTURE

### NATURE OF THE PROBLEM

Electric power is integral to the functioning of electronic components. For highly reliable systems such as commercial and military telecommunications, electric power usually comes from batteries (in the short term), local emergency power supplies (generally over time-intervals of less than 72 hours), and electricity delivered through the local electrical utility (“power” lines in the home, office and factory). Local emergency power supplies are limited by supplies of stored fuel. Increasingly, locally stored fuel in buildings and cities is being reduced for fire safety and environmental pollution reasons, so that the emergency generation availability without refueling is limited.

Geomagnetic storms, a natural phenomenon driven by the solar wind, may, by a different physical mechanism, produce ground-induced currents (GIC) that can affect the electrical system in a manner similar to the E3 component of EMP. Disruptions caused by geomagnetic storms, such as the collapse of Quebec Hydro grid during the geomagnetic storm of 1989, have occurred many times in the past (Figure 5).



Geomagnetic field disturbance conditions,  $dB/dt$  (nT/min) over North America at time 7:45 UT on March 13, 1989

Source: Metatech Corporation, Applied Power Solutions

**Figure 5. Extent of 1989 Geomagnetic Storm**

Depending on the explosive yield of the nuclear weapon used, EMP-induced GIC may be several times larger than that produced by the average geomagnetic storm, and may even be comparable to those expected to arise in the largest geomagnetic storm ever observed. It may also occur over an area not normally affected by historic geomagnetic storms.

The North American economy and the functioning of the society as a whole are critically dependent on the availability of electricity, as needed, where and when needed. The electric power system in the US and interconnected areas of Canada and Mexico is outstanding in terms of its ability to meet load demands with high quality and reliable electricity at reasonable cost. However, over the last decade or two, there has been relatively little large-capacity electric transmission constructed and the generation additions that have been made, while barely adequate, have been increasingly located considerable distances from load for environmental, political, and economic reasons. As a result, the existing National electrical system not infrequently operates at or very near local limits on its physical capacity to move power from generation to load. Therefore, the slightest insult or upset to the system can cause functional collapse affecting significant numbers of people, businesses, and manufacturing. It is not surprising that a single EMP attack may well encompass and degrade at least 70% of the Nation's electrical service, all in one instant.

The impact of such EMP is different and far more catastrophic than that effected by historic blackouts, in three primary respects:

1. The EMP impact is virtually instantaneous and occurs simultaneously over a much larger geographic area. Generally, there are neither precursors nor warning, and no opportunity for human-initiated protective action. The early-time EMP component is the "electromagnetic shock" that disrupts or damages electronics-based control systems and sensors, communication systems, protective systems, and control computers, all of which are used to control and bring electricity from generation sites to customer loads in the quantity and quality needed. The E1 pulse also causes some insulator flashovers in the lower-voltage electricity distribution systems (those found in suburban neighborhoods, in rural areas and inside cities), resulting in immediate broad-scale loss-of-load. Functional collapse of the power system is almost definite over the entire affected region, and may cascade into adjacent geographic areas.
2. The middle-time EMP component is similar to lightning in its time-dependence but is far more widespread in its character although of lower amplitude—essentially a great many lightning-type insults over a large geographic area which might obviate protection. The late-time EMP component couples very efficiently

to long electrical transmission lines and forces large direct electrical currents to flow in them, although they are designed to carry only alternating currents. The energy levels thereby concentrated at the ends of these long lines can become large enough to damage major electrical power system components. The most significant risk is synergistic, because the middle and late-time pulses follow after the early-time pulse, which can impair or destroy protective and control features of the power grid. Then the energies associated with the middle and late-time EMP thus may pass into major system components and damage them. It may also pass electrical surges or fault currents into the loads connected to the system, creating damage in national assets that are not normally considered part of the infrastructure per se. Net result is recovery times of months to years, instead of days to weeks.

3. Proper functioning of the electrical power system requires communication systems, financial systems, transportation systems, and—for much of the generation—continuous or nearly continuous supply of various fuels. However, the fuel-supply, communications, transportation, and financial infrastructures would be simultaneously disabled or degraded in an EMP attack and are dependent upon electricity for proper functioning. For electrical system recovery and restoration of service, the availability of these other infrastructures is essential. The longer the outage, the more problematic, and uncertainty-fraught the recovery will be.

The recent cascading outage of August 14, 2003, is an example of a single failure compounded by system weaknesses and human mistakes. It also provides an example of the effectiveness of protective equipment. However, with EMP there are multiple insults coupled with the disabling of protective devices simultaneously over an extremely broad region—damage to the system is likely and recovery slow.

#### RECOMMENDED MITIGATION AND RESPONSIBILITY

The electrical system is designed to break into “islands” of roughly matching generation and load when a portion of the system receives a severe electrical insult. This serves both to protect electricity supply in the non-impacted regions and to allow for the stable island-systems to be used to “restart” the island(s) that have lost functionality. With EMP, the magnitude, speed, and multi-faceted nature of the insult, its broad geographic reach, along with the number of simultaneous insults, and the adverse synergies all are likely to result in a situation where the islanding scheme will fail to perform as effectively as intended, if at all. Since the impacted geographic area is large, restoring the system from the still-functioning perimeter regions would take a great deal of time, possibly weeks to months at best. Indeed, the only practical way to restart much of the impacted electrical system may be with generation that can be started without an external power source. This is called “black start” generation and primarily includes

hydroelectric (including pumped storage), geothermal, and independent diesel generators of modest capacity.

The recommended actions will substantially improve service and recovery during “normal” large-scale blackouts, and will critically enable recovery under EMP circumstances.

#### PROTECTION

It is impractical to protect the entire electrical power system from damage by an EMP attack. There are too many components of too many different types, manufacturers, designs, and vulnerabilities within too many jurisdictional entities, and the cost to retrofit is too great. Widespread functional collapse of the electrical power system in the area affected by EMP is possible in the face of a geographically broad EMP attack, with even a relatively few unprotected components in place. However, it is practical to reduce to low levels the probability of widespread damage to major power system components that require long times to replace. This will enable significantly improved recovery times, since it avoids the loss of long lead-time and critical components. It is important to protect the ability of the system to fragment gracefully into islands, to the extent practical in the particular EMP circumstance. This approach is cost-efficient and can leverage efforts to improve reliability of bulk electricity supply and enhance its security against the broader range of threats.

***Widespread functional collapse of the electric power system in the area affected by EMP is likely.***

#### RESTORATION

The key to minimizing adverse effects from loss of electrical power is the speed of restoration. Restoration involves matching generation capacity to a load of equivalent size over a transmission network that is initially isolated from the broader system. The larger system is then functionally rebuilt by bringing that mini system, or “island,” to the standard operating frequency and thereupon by adding more blocks of generation and load to this core in amounts that can be absorbed by the growing subsystem. This is a demanding and time-consuming process in the best of circumstances. In the singular circumstance of an EMP attack with multiple damaged components, related infrastructure failures, and particularly severe challenges in communications and transportation, the time required to restore electrical power is expected to be considerably longer than we have experienced in recent history.



However, by protecting key system components needed for restoration, by structuring the network to fail gracefully, and by creating a comprehensive prioritized recovery plan for the most critical power needs, the risk of an EMP attack having a catastrophic effect on the Nation can be greatly reduced. DHS must ensure that the mitigation plan is jointly developed by the federal government and the electric power industry, implemented fully, instilled into systems operations, and tested and practiced regularly to maintain a capability to respond effectively in emergencies. The North American Reliability Council and the Electric Power Research Institute are aptly positioned to provide much of what's needed to support DHS in carrying out its responsibilities. The US Energy Association is well-suited to coordinating activities between and among the various energy sectors that together affect the electric power system and its vitality.

#### ESSENTIAL COMPONENT PROTECTION

1. Assure protection of high-value long-lead-time transmission assets.
2. Assure protection of high-value generation assets. System-level protection assurance is more complex due to the need for multiple systems to function in proper sequence.
3. Assure Key Generation Capability. Not all plants can or should be protected. However, regional evaluation of key generating resources necessary for recovery should be selected and protected.
  - a. Coal-fired generation plants make up nearly half the Nation's generation and are generally the most robust overall to EMP, with many electromechanical controls still in operation. Such coal plants also normally have at least a few days to a month of on-site fuel storage.
  - b. Natural gas-fired combustion turbines and associated steam secondary systems represent the newest and a significant contributor to meeting loads. These have modern electronics-based control and thus are more vulnerable. Natural gas is not stored on-site and likely will be interrupted in an EMP attack. However, provision can be made to have gas-fired plants also operate on fuel oil; many do already.
  - c. Nuclear plants produce roughly 20% of the Nation's generation and have many redundant fail-safe systems that tend to remove them from service whenever any system upset is sensed. Their safe shut down should be assured, but they will be unavailable until near the end of restoration.
  - d. Hydroelectric power is generally quite robust to EMP, and constitutes a substantial fraction of total national generation capacity, albeit unevenly distributed geographically.

- e. In general, the various distributed and renewable fueled generators are not significant enough at this time to warrant special protection.
  - f. Black start generation of all types is critical and will need to be protected from EMP upset or damage.
4. Assure functional integrity of critical communications channels. The most critical communications channels in the power grid are the ones that enable recovery from collapse, such as ones that enable manual operation and coordination-supporting contacts between distant system operators and those that support system diagnostics. Generation, switching, and load dispatch communications support is next in importance.
  5. Assure availability of emergency power at critical facilities needed for restoration. Transmission substations need uninterruptible power to support rapid restoration of grid connectivity and operability, and thereby to more quickly restore service. Most have short-life battery backup systems, but relatively few have longer-duration emergency generators; much more emphasis on the latter is needed.
  6. Assure protection of fuel production and its delivery for generation. Fuel supply adequate to maintain critical electrical service and to restore expanded service is critical. See Fuel/Energy Infrastructure, page 35) for details.
  7. Expand and assure intelligent islanding capability. The ability of the larger electrical power system to break into relatively small subsystem islands is important to mitigate overall EMP impacts and provide faster restoration.
  8. Develop and deploy system test standards and equipment. Device-level robustness standards and test equipment exist, but protection at the system level is the overarching goal. System-level robustness improvements such as isolators, line protection, and grounding improvements will be the most practical and least expensive in most cases relative to replacement with more robust individual component devices. Periodic testing of system response is necessary.

## SYSTEM RESTORATION

1. Develop and enable a restoration plan. This plan must prioritize the rapid restoration of power to government-identified critical service. Sufficient black start generation capacity must be provided where it is needed in the associated subsystem islands, along with transmission system paths that can be isolated and connected to matching loads. The plan must address outages with wide geographic coverage, multiple major component failures, poor communication capabilities, and widespread failure of islanding schemes within the EMP-affected area. Government and industry responsibilities must be unequivocally and completely assigned. All necessary legal and financial arrangements, e.g., for indemnification, must be put into place to allow industry to implement specified government priorities with respect to service restoration, as well as to deal with potential environmental and technical hazards in order to assure rapid recovery.

2. Simulate, train, exercise, and test the plan. Simulators must be developed for use in training and developing procedures similar to those in the airline industry; a handful should suffice for the entire country. Along with simulation and field exercises, Red Team discipline should be employed to surface weaknesses and prioritize their rectification.
3. Assure sufficient numbers of adequately trained recovery personnel.
4. Assure availability of replacement equipment. R&D is under way—and should be vigorously pursued—into the production of emergency “universal” replacements. The emergency nature of such devices would trade efficiency and service-life for modularity, transportability, and affordability.
5. Implement redundant backup diagnostics and communication. Assure that system operators can reliably identify and locate damaged components.

## TELECOMMUNICATIONS

### IMPORTANCE OF ASSURED TELECOMMUNICATIONS

Telecommunications plays a key role in US society in terms of its direct effect on individuals and business and due to its impact on other key infrastructures. The relationship of telecommunications to the other critical infrastructures, such as the financial industry, is often recognized during and following widespread outages, such as those experienced as a result of the September 11, 2001, attacks on the World Trade Centers and the immediate vicinity of “Ground Zero.” The local disruption of all critical infrastructures, including power, transportation, and telecommunications, interrupted operations in key financial markets and posed increased liquidity risks to the US financial system.<sup>1</sup> In the days following the attacks, institutions in the affected areas were implementing their business continuity plans, which proved vital to the rapid restoration and recovery of services in the New York City area. In addition, the President emphasized that the prompt restoration of Wall Street’s capabilities was critical to the economic welfare of the Nation; in doing so, he aptly linked economic stability to national security.

For some of the most critical infrastructure services, such as electric power, natural gas, and financial services, assured communications are essential to their recovery following a major adverse event. The importance of telecommunications in an emergency situation is underscored by the existence of the National Communications System (NCS), established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*,<sup>2</sup> which include administering the National

---

<sup>1</sup> James J. MacAndrews and Simmon M. Potter, “Liquidity Effects of the Events of September 11, 2001,” Federal Reserve Bank of New York Economic Policy Review, November 2002.

<sup>2</sup> The mission of the NCS shall be to assist the President, the National Security Council, the Homeland Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget in: (1) the exercise of the telecommunications functions and responsibilities set forth in Section 2 of this Order; and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.

The NCS shall seek to ensure that a national telecommunications infrastructure is developed which: (1) Is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies and other entities, including telecommunications in support of national security leadership and continuity of government; (2) Is capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources; (3) Incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain, to the maximum extent

Coordinating Center (NCC) for Telecommunications to facilitate the initiation, coordination, restoration, and reconstitution of National Security and Emergency Preparedness (NS/EP) telecommunications services or facilities under all crises and emergencies; developing and ensuring the implementation of plans and programs that support the viability of telecommunications infrastructure hardness, redundancy, mobility, connectivity, and security; and serving as the focal point for joint industry-government and interagency NS/EP telecommunications planning and partnerships. In addition, the President's National Security Telecommunications Advisory Committee (NSTAC), a Federal Advisory Committee Act (FACA) CEO-level advisory group to the President, is tasked with providing industry-sourced advice and expertise related to implementing policies affecting NS/EP communications. These NS/EP services are those "critical to the maintenance of a state of readiness or the response to and management of any event or crisis that causes harm or could cause harm to the population, damage to or the loss of property, or degrades or threatens the NS/EP posture of the United States."<sup>3</sup>

The NSTAC in its 1985 Report on EMP found that "consistent with its cost constraints, industry should incorporate low-cost EMP mitigation practices into new facilities and, as appropriate, into upgrade programs. For those areas where a carrier/supplier recognizes that a significant improvement in EMP resistance and surveillance could be achieved, but at a cost beyond the carrier/supplier's own cost constraints, the carrier/supplier should identify such options to the government for evaluation and possible funding." On October 9, 1985, the NSTAC approved the EMP Final Task Force Report and forwarded a recommendation to the President, calling for a joint industry and Government program to reduce the costs of existing techniques for mitigating high-altitude electromagnetic pulse (HEMP)-induced transients and to develop new techniques for limiting transient effects. As a result, the NCS and industry, working with the ATIS—the Alliance for Industry Solutions—developed a set of ANSI standards and Generic Requirements<sup>4</sup> to address EMP.<sup>5</sup>

---

practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency; and (4) Is consistent, to the maximum extent practicable, with other national telecommunications policies.

<sup>3</sup> NS/EP Implications for Electronic Commerce, NSTAC Report, June 1999.

<sup>4</sup> Telcordia GR-1089-CORE.

<sup>5</sup> ANSI T1.320.



### NS/EP Definitions

***NS/EP Telecommunications Services:*** Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrades or loss of property, or degrades or threatens the NS/EP posture of the United States. (*“Telecommunications Service Priority [TSP] System for National Security Emergency Preparedness: Service User Manual,” NCS Manual 3-1-1, July 9, 1990. Appendix A.*)

***NS/EP Requirements:*** Features that maintain a state of readiness or respond to and manage an event or crisis (local, national, or international), which causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the NS/EP posture of the United States. (*Federal Standard 1037C*)

With respect to NS/EP telecommunications, capabilities exist for prioritizing phone calls through the wireline, wireless, and satellite networks during the time interval when call volumes are excessive and facilities are damaged, giving priority to restoring services that may be damaged or degraded, and getting new circuits into operation.

According to recent testimony by a DHS official, “The NCS is continuing a diverse set of mature and evolving programs designed to ensure priority use of telecommunications services by NS/EP users during times of national crisis. The more mature services—including the Government Emergency Telecommunications Service (GETS) and the Telecommunications Service Priority (TSP)—were instrumental in the response to the September 11 attacks. FY 2005 funding enhances these programs and supports the development of the Wireless Priority Service (WPS) program and upgrade to the Special Routing Arrangement Service (SRAS). Specifically, priority service programs include: (1) GETS, which offers nationwide priority voice and low-speed data service during an emergency or crisis situation; (2) WPS, which provides a nationwide priority cellular service to key NS/EP users, including individuals from federal, state and local governments and the private sector; (3) TSP, which provides the administrative and operational framework for priority provisioning and restoration of critical NS/EP telecommunications services; (4) SRAS, which is a variant of GETS to support the Continuity of Government (COG) program including the reengineering of SRAS in the AT&T network and development of SRAS capabilities in the MCI and Sprint networks, and; (5) the Alerting and Coordination Network (ACN), which is an NCS program that

provides dedicated communications between selected critical government and telecommunications industry operations centers.”<sup>6</sup>

For example, due to concerns with respect to getting calls through during intervals of high network call volumes that follow disaster events, the Nuclear Regulatory Commission (NRC) utilizes the Government Emergency Telecommunications System (GETS) and other NS/EP telecom services such as wireless priority services to communicate with commercial nuclear power plants and to relay critical status information. This use of GETS grew out of lessons learned from the Three Mile Island incident in 1979. During the initial days of this incident, NRC personnel experienced communication problems that were attributed primarily to call volume overload at the local telephone company switch.

Another NS/EP service is the Telecommunications Service Priority (TSP) program, which exists to assign priority provisioning and restoration of critical NS/EP telecommunications services in the hours immediately following a major disaster. In place since the mid-1980s, more than 50,000 circuits are protected today under TSP, including circuits associated with critical infrastructures such as electric power, telecommunications, and financial services.

The telecommunication system consists of four basic and primary physical systems: wireline, wireless, satellite, and radio. In general, the national telecommunications infrastructure may be farther advanced than others in its ability to address the particular consequences of EMP. This is due in large measure to the recognized alternative threats to this system, as well as broad recognition of its importance to society. The three primary and separate systems (excluding radio) that make up the broad telecommunications infrastructure each provide specialized services; they also overlap heavily. Thus the loss or degradation of any one of these somewhat redundant subsystems subjects the remaining functional subsystems to heavier service loads.

Each of these four primary systems is unique in their capability to suffer insult from EMP. The wireline system is robust but will be degraded within the area exposed to the EMP electromagnetic fields. The wireless system is technologically fragile in relation

---

<sup>6</sup> Statement of General Frank Libutti, Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, Before the House Homeland Select Subcommittee on Intelligence and Counterterrorism and the Subcommittee on Infrastructure and Border Security, March 4, 2004, p. 12.

to EMP, certainly in comparison to the wireline one. In general, it may be so seriously degraded in the EMP region as to be unavailable. Low Earth Orbit (LEO) communications satellites may also suffer radiation damage as a result of one or more high-altitude nuclear bursts that produce EMP (see Space Systems, page 44).

The radio communication sub-system of the national telecommunications infrastructure is not widespread, but where it is connected to antennas, power lines, telephone lines, or other extended conductors, it is also subject to substantial EMP damage. However, radio communication devices not so connected or not connected to such conductors at the time of the EMP attack are likely to be operable in the post-attack interval.

#### EMP EFFECTS ON TELECOMMUNICATIONS

Based upon results of Commission-sponsored testing, an EMP attack would disrupt or damage a functionally significant fraction of the electronic circuits in the Nation's civilian telecommunications systems in the region exposed to EMP. The remaining operational networks would be subjected to high levels of call attempts for some period of time after the attack, leading to degraded telecommunications services.

Key government and civilian personnel will need priority access to use public network resources to coordinate and support local, regional, and national recovery efforts, especially during the interval of severe network congestion.

To offset the temporary loss of electric power, telecommunications sites now utilize a mix of batteries, mobile generators, and fixed-location generators. These typically have between 4 and 72 hours of backup power available, and thus will depend on either the resumption of electrical utility power or fuel deliveries to function for longer periods of time.

For some of the most critical infrastructure services such as electric power, natural gas, and financial services, assured communications are necessary—but aren't necessarily sufficient—to the survival of that service during the initial time-intervals after an EMP attack. Therefore, a systematic approach to protecting or restoring key communications systems will be required.

#### RECOMMENDED MITIGATION ACTIVITIES

The following actions are recommended as particularly effective ones for mitigating the impacts of EMP attack:

- Expand the respective roles of the National Communications System (NCS) and the Defense Threat Reduction Agency (DTRA) as the Federal Focal Point for EMP within the Code of Federal Regulations Part 215<sup>7</sup> to address infrastructure interdependencies related to NS/EP telecommunications services.
- Ensure services targeted at NS/EP operate effectively as new technology is introduced into the telecommunications network. Specifically, services such as Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) that are intended for use in emergency situations to improve the call completion probabilities for key personnel must operate effectively. Within the next 15 years, new technologies will be introduced into the public networks that will play major roles in operation of these services. EMP is just one of the potential threats that could stress the telecommunications networks; therefore, ensuring that NS/EP services perform effectively as new technology is introduced has benefits beyond providing robustness to EMP, and moreover is consistent with avoiding failures from other hostile actions.
- Determine the effects of EMP on different types of telecommunication equipment and facilities, using tests and theoretical analyses of the type done in the course of Commission-sponsored work and previous EMP-related studies conducted by the National Communications System (NCS).<sup>8</sup> A comprehensive, continuing telecommunications testing program,<sup>9</sup> along with the use of existing national and international standards,<sup>10</sup> may be a model activity that would be a key part of this overall National effort.
- Improve the ability of key network assets to survive HEMP. There are key elements in the network such as the Signal Transfer Points (STPs) in the signaling system (Signaling System 7 (SS7)), Home Location Register (HLR), and Visiting Location Register (VLR) in the wireless networks whose degradation can result in the loss of service to a larger number of users. Effective mitigation strategies include a combination of site hardening and installation of protective measures for the fast rise-time (E1) component of EMP.
- Improve the ability of telecommunications to withstand the sustained loss of utility-supplied electric power. This mitigation strategy would entail the use of best practices, review and improvement of existing programs such

---

<sup>7</sup> 47CFR, Section 215, designated The Executive Agent, NCS, is the focal point within the Federal Government for all EMP technical data and studies concerning NS/EP telecommunications.

<sup>8</sup> For example: The Effects of High-Altitude Electromagnetic Pulse (HEMP) on Telecommunications Assets, NCS Technical Information Bulletin 92-5, February 1992.

<sup>9</sup> Similar to that conducted in response to the Signaling System 7 outages of the early 1990's (which affected large portions of the United States) under the Inter-network Interoperability Test Program (IITP) of the Alliance for Telecommunications Industry Solutions (ATIS).

<sup>10</sup> Standards for Protection of Telecommunications Links, NCS Technical Notes, Volume 6, Number 3, 1999.

as the Telecommunications Electric Service Priority (TESP) program, and the increased use of alternative backup power sources.

- Conduct exercises to refine contingency operations. Conduct exercises that test and provide for improved contingency operations, assuming widespread multi-infrastructure degradation. The adequacy of mutual aid agreements, cross-organizational planning and coordination, and critical asset prioritization are examples of elements that should be tested and developed.
- Managers of these critical services must design their systems and operating procedures to take into account the potential vulnerabilities introduced by EMP-driven failure of telecommunications devices and sub-systems.



## BANKING AND FINANCE

### NATURE OF THE PROBLEM

The financial services industry comprises a network of organizations and attendant systems that process instruments of monetary value in the form of deposits, loans, funds transfers, savings, and other financial transactions. It includes banks and other depository institutions, including the Federal Reserve System; investment-related companies such as underwriters, brokerages, and mutual funds; industry utilities such as the New York Stock Exchange, the Automated Clearing House, and the Society for Worldwide Interbank Financial Telecommunications; and third party processors that provide electronic processing services to financial institutions, including data and network management and check processing.

Virtually all American economic activity depends upon the functioning of the financial services industry. Today, most financial transactions that express National wealth are performed and recorded electronically. Virtually all transactions involving banks and other financial institutions happen electronically. Essentially all record-keeping of financial transactions involves information stored electronically. The financial services industry has evolved to the point that it would be impossible to operate without the efficiencies, speeds, and processing and storage capabilities of electronic information technology.

The terrorist attacks of September 11, 2001, demonstrated the vulnerabilities arising from the significant interdependencies of the Nation's critical infrastructures. The attacks disrupted all critical infrastructures in New York City, including power, transportation, and telecommunications. Consequently, operations in key financial markets were interrupted, increasing liquidity risks for the United States financial system.<sup>11</sup>

The Interagency Paper,<sup>12</sup> which was jointly issued by the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), and the Securities and Exchange Commission (SEC), specifies clearing and settlement systems as the most

<sup>11</sup> James J. MacAndrews and Simmon M. Potter, "Liquidity Effects of the Events of September 11, 2001," Federal Reserve Bank of New York Economic Policy Review, November 2002.

<sup>12</sup> The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System*, September 5, 2002.

critical business operations at risk for financial markets.<sup>13</sup> Because financial markets are highly interdependent, a wide-scale disruption of core clearing and settlement processes would have an immediate systemic effect on critical financial markets.<sup>14</sup>

*Over the past couple of decades, the American economy has become increasingly resilient to shocks. Deregulated financial markets, far more flexible labor markets, and, more recently, the major advances in information technology have enhanced our ability to absorb disruptions and recover. In the past, our economy has quickly regained its previous levels following the devastation of hurricanes, earthquakes, floods, and myriad other natural disasters that periodically batter various regions of our country. Although the trauma of September 11 shares some characteristics with such disruptions, the differences are important. In contrast to natural disasters, last week's events are of far greater concern because they strike at the roots of our free society, one aspect of which is our market-driven economy. All modern economies require the confidence that free-market institutions are firmly in place and that commitments made today by market participants will be honored not only tomorrow, but for years into the future. The greater the degree of confidence in the state of future markets, the greater the level of long-term investment. The shock of September 11, by markedly raising the degree of uncertainty about the future, has the potential to result, for a time, in a pronounced disengagement from future commitments. And that, in the short run, would imply a lessened current level of activity. Indeed, much economic activity ground to a halt last week. But the foundations of our free society remain sound, and I am confident that we will recover and prosper as we have in the past. As a consequence of the spontaneous and almost universal support that we received from around the world, an agreement on a new round of multilateral trade negotiations now seems more feasible. Such an outcome would lead to a stronger global market system. A successful round would not only significantly enhance world economic growth but also answer terrorism with a firm reaffirmation of our commitment to open and free societies.*

—Testimony of Chairman Alan Greenspan, *The condition of the financial markets* Before the Committee on Banking, Housing, and Urban Affairs, US Senate September 20, 2001

Moreover, in December 2002, the FRB revised its policy and procedures for NS/EP telecommunications programs administered by the National Communications System (NCS) to identify those functions supporting the Federal Reserve's NS/EP mission to maintain national liquidity.<sup>15</sup> The FRB expanded the scope of services that would seriously affect continued financial operations if a telecommunications disruption

<sup>13</sup> Ibid., pg. 5.

<sup>14</sup> Systemic risk includes the risk that the failure of one participant in a transfer system or financial market to meet its required obligations will cause other participants to be unable to meet their obligations when due, causing significant liquidity or credit problems or threatening the stability of financial markets. The use of the term "systemic risk" in this report is based on the international definition of systemic risk in payments and settlement systems provided in Committee on Payment and Settlement Systems, Bank for International Settlements, "A Glossary of Terms in Payment and Settlement Systems," 2001.

<sup>15</sup> *Federal Register*, vol. 67, no. 236, Monday, December 9, 2002. Notice, "Federal Reserve Board Sponsorship for Priority Telecommunication Services of Organizations That Are Important to National Security/ Emergency Preparedness," <http://www.federalreserve.gov/boarddocs/press/other/2002/20021203/attachment.pdf>.

of “a few minutes to one day” occurred.<sup>16</sup> These functions, which are listed below, require same-day recovery and are critical to the operation and liquidity of banks and the stability of financial markets:

- Large-value inter-bank funds transfer, securities transfer, or payment-related services, such as Fedwire, Clearing House Interbank Payments System (CHIPS), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT)
- Automated clearinghouse (ACH) operators
- Key clearing and settlement utilities
- Treasury automated auction and processing system
- Large-dollar participants of these systems and utilities

The increasing dependence of the United States on an electronic economy, so beneficial to the creation and preservation of wealth, also adds to the adverse effects that would be produced by an EMP attack. The electronic technologies that are the foundation of the financial infrastructure are potentially vulnerable to EMP. These systems are also potentially vulnerable to EMP indirectly through other critical infrastructures, such as the electric power grid and telecommunications.

#### RECOMMENDED MITIGATION AND RESPONSIBILITY

Securing the financial services industry from the EMP threat is vital to the national security of the United States. The Federal government must assure that this system can survive sufficiently to preclude serious, long-term consequences.

The Department of Homeland Security, the Federal Reserve Board, and the Department of the Treasury, in cooperation with other relevant agencies, must develop contingency plans to ride out and recover key financial systems promptly from an EMP attack.

Key financial services include those means and resources that provide the general population with cash, credit, and other liquidity required to buy food, fuel, and other essential goods and services. We must protect the Nation’s financial networks, banking records, and data retrieval systems that support cash, check, credit, debit, and other transactions through judicious balance of hardening, redundancy, and contingency plans.

---

<sup>16</sup> Federal Reserve Board Sponsorship for Priority Telecommunications Services of Organizations That Are Important to National Security/Emergency Preparedness, *Federal Register*, Vol. 67, No. 236, Monday, December 2003, Notices, p. 72958.

The Federal government must work with the private sector to assure the protection and effective recovery of essential financial records and services infrastructure components from all deliberate adverse events, including EMP attack. Implementation of the recommendations made by the Department of the Treasury, the FRB, and the SEC in their *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System* to meet sabotage and cyber-threats that could engender requirements for protection and recovery should be expanded to include expeditious recovery from EMP attack:

- “Every organization in the financial services industry should identify all clearing and settlement activities in each critical financial market in which it is a core clearing and settlement organization or plays a significant role” that could be threatened by EMP attack.
- Industry should “determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets” following an EMP attack.
- Industry should be prepared to cope with an EMP attack by maintaining “sufficient geographically dispersed resources to meet recovery and resumption objectives.... Backup sites should not rely on the same infrastructure components (e.g., transportation, telecommunications, water supply, electric power) used by the primary site. Moreover, the operation of such sites should not be impaired by a wide-scale evacuation at or inaccessibility of staff that service the primary site.”
- Industry should, “Routinely use or test recovery and resumption arrangements.... It is critical for firms to test backup facilities of markets, core clearing and settlement organizations, and third-party service providers to ensure connectivity, capacity, and the integrity of data transmission” against an EMP attack.

## FUEL/ENERGY INFRASTRUCTURE

The vulnerabilities of this sector are produced by the responses of the electronic control systems that provide and utilize the near-real-time data flows needed to operate the fuel/energy infrastructure efficiently, as well as to identify and quickly react to equipment malfunctions or untoward incidents. EMP could also cause control or data-sensor malfunctions that are not easily discernible, leading to counterproductive operational decisions. Process control systems are critical to the operation and control of petroleum refineries, and little or no notice of an outage significantly increases the potential for damage during an emergency shutdown. Communications systems that are critical for operational control represent another locus of vulnerability. Communications are also critical in refineries to ensure safety of on-site personnel, the adjacent population, and the surrounding environment. The energy distribution infrastructure is also critically dependent on the availability of commercial power to operate the numerous pumps, valves and other electrical equipment that are required for a functional infrastructure.

DHS must develop a contingency plan that will provide strategy for protection and recovery for this sector, to include actions to be taken by both Government and industry. Government should establish a national inventory of parts for those items with long lead-times or that would be in demand in the event of a catastrophic event such as an EMP attack. The Energy Information Sharing and Analysis Center (ISAAC) should, with government funding, expand its mission to address EMP issues, and the government should work with the private sector to implement the general approach described in Strategy and Recommendations, page 11.



## TRANSPORTATION INFRASTRUCTURE

### NATURE OF THE PROBLEM

America's transportation sector is often addressed as a single infrastructure, but in reality its multiple modes provide for several separate infrastructures. Rail includes the freight railroad and commuter rail infrastructures; road includes the trucking and automobile infrastructures; water includes the maritime shipping and inland waterway infrastructures; and air includes the commercial and general aviation infrastructures.

As recognized by the President's National Security Telecommunications Advisory Committee (NSTAC) Information Infrastructure Group Report:<sup>17</sup>

- The transportation industry is increasingly reliant on information technology and public information-transporting networks.
- Although a nationwide disruption of the transportation infrastructure may be unlikely, even a local or regional disruption could have a significant impact. Due to the diversity and redundancy of the US transportation system, the infrastructure is not at risk of nationwide disruption resulting from information system failure. Nonetheless, a disruption of the transportation information infrastructure on a regional or local scale has potential for widespread economic and national security effects.
- Marketplace pressures and increasing utilization of IT make large-scale, multimodal disruptions more likely in the future. As the infrastructure becomes more interconnected and interdependent, the transportation industry will increasingly rely on information technology to perform its most basic business functions. As this occurs, it becomes more likely that information system failures could result in large-scale disruptions of multiple modes of the transportation infrastructure.
- There is a need for a broad-based infrastructure assurance awareness program to assist all modes of transportation.
- The transportation industry could leverage ongoing research and development initiatives to improve the security of the transportation information infrastructure.

***Electronics vulnerable to EMP permeate the transportation infrastructures.***

<sup>17</sup> NSTAC Information Infrastructure Group Report, June 1999, <<http://www.ncs.gov/NSTAC/NSTACXXII/Reports/NSTAC22-IIIG.pdf>>.

- There is a need for closer coordination between the transportation industry and other critical infrastructures.

The imperative to achieve superior performance has also led to a tremendous increase in the use of electronics that are potentially vulnerable to EMP. The internal combustion engine provides a familiar example of this phenomenon. Modern engines utilize electronics to increase performance, increase fuel efficiency, reduce emissions, increase diagnostic capability, and increase safety.

To gauge the degree of vulnerability of transportation infrastructures to EMP, the Commission has conducted an assessment of selected components of these infrastructures that are necessary to their operations. The assessment relied on testing where feasible, surveys and analyses for equipment and facilities for which testing was impractical, and reference to similarities to equipment for which EMP vulnerability data exists.

Based on this assessment, significant degradation of the transportation infrastructures are likely to occur in the immediate aftermath of an EMP attack. For example, municipal road traffic will likely be severely congested, possibly to the point of wide-area gridlock, as a result of traffic light malfunctions and the fraction of operating cars and trucks that will experience both temporary and in some cases unrecoverable engine shutdown. Railroad traffic will stop if communications with railroad control centers are lost or railway signals malfunction. Commercial air traffic will likely cease operations for safety and other traffic control reasons. Ports will stop loading and unloading ships until commercial power and cargo hauling infrastructures are restored.

The ability of the major transportation infrastructure components to recover depends on the plans in place and the availability of resources—including spare parts and support from other critical infrastructures upon which transportation is dependent. Transportation infrastructures have emergency response procedures in place; however, they do not explicitly address conditions that may exist for an EMP attack, such as little or no warning time and simultaneous disruptions over wide areas. Restoration times will depend on the planning and training carried out, and on the availability of services from other infrastructures—notably power, fuel, and telecommunications.

## STRATEGY FOR PROTECTION AND RECOVERY

### *RAILROADS*

Railroad operations are designed to continue under stressed conditions. Backup power and provisioning is provided for operations to continue for days or even weeks at reduced capacity. However, some existing emergency procedures, such as transferring

operations to backup sites, rely on significant warning time, such as may be received in a weather forecast before a hurricane. An EMP attack may occur without warning, thereby compromising the viability of available emergency procedures. Therefore, under the overall leadership of the DHS, the government and private sectors should work together to implement the general approach described in Strategy and Recommendations, page 11.

Specific actions should include:

- Heighten railroad officials' awareness of the possibility of EMP attack without warning that would produce wide-area, long-term disruption and damage to electronic systems.
- Perform test-based EMP assessments of railroad traffic control centers and retrofit modest EMP protection into these facilities, thereby minimizing the potential for adverse long term EMP effects. The emphasis of this effort should be on electronic control and telecommunication systems.

#### *TRUCKING AND AUTOMOBILES*

Emphasizing prevention and emergency clearing of traffic congestion in this area, DHS should coordinate a government and private sector program to:

- Initiate an outreach program to educate State and local authorities and traffic engineers on EMP effects and the expectation of traffic signal malfunctions, vehicle disruption and damage, and consequent traffic congestion.
- Work with municipalities to formulate recovery plans, including emergency clearing of traffic congestion and provisioning spare controller cards that could be used to repair controller boxes.
- Sponsor development of economical protection modules—preliminary results for which are already available from Commission-sponsored research—that could be retrofitted into existing traffic signal controller boxes and installed in new controller boxes during manufacture.
- Sponsor development of automobile robustness specifications and testing for EMP. These specifications should be implemented by augmenting existing specifications for gaining immunity to transient electromagnetic interference (EMI), rather than by developing separate specifications for EMP.

#### *MARITIME SHIPPING*

The essential port operations to be safeguarded are ship traffic control, cargo loading and unloading, and cargo storage and movement (incoming and outgoing). Ship traffic control is provided by the Coast Guard, which has robust backup procedures in

place. Cargo storage and movement are covered by other transportation infrastructure recommendations. Therefore, focusing on cargo operations in this area, DHS should coordinate a government and private sector program to:

- Heighten port officials' awareness of the wide geographic coverage of EMP fields, the risk due to loss of commercial power for protracted time-intervals, and the need to evaluate the practicality of providing emergency generators for at least some portion of port and cargo operations.
- Assess the vulnerability of electric-powered loading/unloading equipment. Review the electromagnetic protection already in place for lightning, and require augmentation of this protection to provide significant EMP robustness.
- Coordinate findings with the "real-time" repair crews to ensure they are aware of the potential for EMP damage. Based on the assessment results, recommend spares provisions so that repairs can be made in a timely manner.
- Assess port data centers for the potential loss of data in electronic media. Provide useful measures of protection against EMP causing loss of function and/or data.
- Provide protected off-line spare parts and computers sufficient for minimum essential operations.
- Provide survivable radio and satellite communication capabilities for the Coast Guard and the Nation's ports.

#### *COMMERCIAL AVIATION*

In priority order, it must be ensured that airplanes caught in the air during an EMP attack can land safely, that critical recovery assets are protected, and that contingency plans for an extended no-fly period are developed. Thus, DHS should coordinate a government program in cooperation with the FAA to perform an operational assessment of the air traffic control system to identify a "thin-line" that provides the minimal essential capabilities necessary to return the air traffic control capability to at least a basic level of service after an EMP attack. Based on the results of this operational assessment, develop tactics for protection, operational workarounds, spares provisioning, and repairs to return to a minimum-essential service level.

## FOOD INFRASTRUCTURE

### NATURE OF THE PROBLEM

EMP can damage or disrupt the infrastructure that supplies food to the population of the United States. Recent federal efforts to better protect the food infrastructure from terrorist attack tend to focus on preventing small-scale disruption of the food infrastructure, such as would result from terrorists poisoning some food. Yet an EMP attack could potentially disrupt the food infrastructure over a large region encompassing many cities for a protracted period of weeks to months.

Technology has made possible a dramatic revolution in US agricultural productivity. The transformation of the United States from a nation of farmers to a nation where less than 2 percent of the population is able to feed the other 98 percent and supply export markets is made possible only by technological advancements that, since 1900, have increased the productivity of the modern farmer by more than 50-fold. Technology, in the form of knowledge, machines, modern fertilizers and pesticides, high-yield crops and feeds, is the key to this revolution in food production. Much of the technology for food production directly or indirectly depends upon electricity, transportation, and other infrastructures.

The distribution system is a chokepoint in the US food infrastructure. Supermarkets typically carry only enough food to provision the local population for 1 to 3 days. Supermarkets replenish their stocks on virtually a daily basis from regional warehouses that usually carry enough food to supply a multi-county area for about one month. The large quantities of food kept in regional warehouses will do little to alleviate a crisis if it cannot be distributed to the population in a timely manner. Distribution depends largely on a functioning transportation system.

### MITIGATION AND RESPONSIBILITY

Federal, state, and regional governments should establish plans for assuring that food is available to the general population in case of major disruption of the food infrastructure. Planning to locate, preserve, deliver, distribute, and ration existing stockpiles of processed and unprocessed food, including food stockpiled by the Department of Agriculture, Department of Defense, and other government agencies, will



be an important component of maintaining the food supply. Planning to protect, deliver, and ration food from regional warehouses, under conditions where an EMP attack has disrupted the power, transportation, and other infrastructures for a protracted period, should be a priority. Plans to process and deliver private and government grain stockpiles would significantly supplement the processed food stored in regional warehouses. According to the USDA's National Agricultural Statistical Service, total private grain stockpiles in the United States amount to over 255 million metric tons. Federal grain stockpiles held by the Commodity Credit Corporation exceed 1.7 million metric tons, with 1.6 million metric tons of that amount dedicated to the Bill Emerson Humanitarian Trust for Overseas Emergency. Planning should include an assessment of how much food the population of the United States would need in an emergency when the food infrastructure is disrupted for a protracted period. Food stockpiles should be increased if existing stockpiles of food appear to be inadequate.

Presidential initiatives have designated the Department of Homeland Security as the lead agency responsible for the security of the food infrastructure, overseeing and working with the Department of Agriculture. Currently, under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act), the President "is authorized and directed to assure that adequate stocks of food will be ready and conveniently available for emergency mass feeding or distribution" in the United States. The Stafford Act should be amended to provide for plans to locate, protect, and distribute existing private and government stockpiles of food, and to provide plans for distribution of existing food stockpiles to the general population in the event of a national emergency.

## WATER SUPPLY INFRASTRUCTURE

National-level responsibilities have already been assigned to the Department of Homeland Security (DHS) and the Environmental Protection Agency (EPA) to protect the water infrastructure from terrorist threats. A recent Presidential Directive establishes new national policy for protection of our Nation's critical infrastructures against terrorist threats that could cause catastrophic health effects.<sup>18</sup> EPA is the designated lead agency for protection of drinking water and water treatment systems. DHS and EPA should ensure that protection includes EMP attack among the recognized threats to the water infrastructure.

---

<sup>18</sup> Homeland Security Presidential Directive – 7, *Critical Infrastructure Identification, Prioritization, and Protection*. December 17, 2003.

## EMERGENCY SERVICES

### VULNERABILITIES

An EMP attack will result in diminished capabilities of emergency services during a time of greatly increased demand upon them. The EMP vulnerability of emergency services systems is primarily due to the susceptibility of computer and communications equipment, and secondarily due to likely commercial electric power outages. Recent test results indicate that some failures of computers and network equipment can be expected at low EMP field levels; at higher levels, much more pervasive equipment failures are expected. Mobile radio communications equipment can be expected to experience disruption and failure at EMP threat levels that are likely to be experienced. Moreover, emergency services are critically dependent on the commercial telephone network, on electric power, and thus on fuel for backup generators. Degradation in these capabilities following an EMP attack is likely, as discussed previously, thereby providing another source of cascading infrastructure failure.

### RECOMMENDED STRATEGY FOR PROTECTION AND RECOVERY

The Department of Homeland Security must develop a strategy for protection and recovery of emergency services that emphasizes the inclusion of the EMP threat in planning and training and the establishment of technical standards for EMP protection of critical equipment. The Department of Homeland Security, including its Federal Emergency Management Agency (FEMA), and state and local governments should augment existing plans and procedures to address both immediate and long-term emergency services response to EMP attack. Plans should include provision for early warning notification, and a protection/recovery protocol based on graceful degradation and rapid recovery that emphasizes a balance between limited hardening and provisioning of spare components, as well as training for their use in emergency reconstitution. In addition, the Department of Homeland Security should provide technical support, guidance, and assistance to state and local governments, as well as to other federal departments and agencies, to ensure the EMP survivability or rapid recovery of critical emergency services networks and equipment.

## SPACE SYSTEMS

Over the past few years, there has been increased focus on US space systems in low Earth orbits and their unique vulnerabilities, among which is their susceptibility to nuclear detonations at high altitudes—the same events that produce EMP. It is also important to include, for the protection of a satellite-based system in any orbit, its control system and ground infrastructure, including up-link and down-link facilities.

Commercial satellites support many significant services for the Federal government, including communications, remote sensing, weather forecasting, and imaging. The national security and homeland security communities use commercial satellites for critical activities, including direct and backup communications, emergency response services, and continuity of operations during emergencies. Satellite services are important for national security and emergency preparedness telecommunications because of their ubiquity and separation from other communications infrastructures.

The Commission to Assess United States National Security Space Management and Organization conducted an assessment of space activities that support US national security interests, and concluded that space systems are vulnerable to a range of attacks due to their political, economic, and military value.<sup>19</sup> Satellites in low Earth orbit generally are at very considerable risk of severe lifetime degradation or outright failure from collateral radiation effects arising from an EMP attack on ground targets.

The Department of Homeland Security and the Department of Defense should jointly execute a systematic assessment of the significance of each space system, particularly those in low Earth orbits, to missions such as the continuity of government, strategic military force protection, and the protection of critical tactical force support functions. Information from this assessment and associated cost and risk judgments will inform senior government decision making regarding protection and performance-assurance of these systems, so that missions can be executed with the required degrees of surety in the face of the possible threats.

---

<sup>19</sup> *Report of the Commission to Assess United States National Security Space Management and Organization*, January 11, 2001.

## GOVERNMENT

DHS should give priority to measures to ensure that the President and other senior Federal officials can exercise informed leadership of the Nation in the aftermath of an EMP attack, and to improving post-attack response capabilities at all levels of government.

The President, Secretary of Homeland Security, and other senior officials must be able to manage the national recovery in an informed and reliable manner. Current national capabilities were developed for Cold War scenarios in which it was imperative that the President have assured connectivity to strategic retaliatory forces. While this is still an important requirement, there is a new need for considerably broader, robust connectivity between national leaders, government at all levels, and key organizations within each infrastructure sector so that the status of infrastructures can be assessed in a reliable and comprehensive manner and their recovery and reconstitution intelligently managed. The Department of Homeland Security, working through the Homeland Security Council, should give high priority to identifying and achieving the minimum levels of robust connectivity needed for recovery following EMP attack. In doing this, DHS should give particular emphasis to exercises that evaluate the robustness of the solutions being implemented.

Working with state authorities and private-sector organizations, the Department of Homeland Security should develop draft protocols for implementation by emergency and other government responders following EMP attack, Red Team these extensively, and then institutionalize validated protocols through issuance of standards, training, and exercises.



## KEEPING THE CITIZENRY INFORMED

Support to National leadership also involves measures to ensure that the President can communicate effectively with the citizenry. Although the US can improve prevention, protection, and recovery in the face of an EMP attack to levels below those that would have catastrophic consequences for the Nation, an EMP attack would still cause substantial disruption, even under the best of circumstances. Many citizens would be without power, communications and other services for days—or perhaps substantially longer—before full recovery could occur. During that interval, it will be crucial to provide a reliable channel of information to those citizens to let them know what has happened, the current situation, when help of what types for them might be available, what their governments are doing, and the host of questions which, if not answered, are certain to create more instability and suffering for the affected individuals, communities, and the Nation as a whole.

## PROTECTION OF MILITARY FORCES

The end of the Cold War relaxed the discipline for achieving EMP survivability within the Department of Defense, and gave rise to the perception that an erosion of EMP survivability of military forces was an acceptable risk. EMP simulation and test facilities have been mothballed or dismantled, and research concerning EMP phenomena, hardening design, testing, and maintenance has been substantially decreased. However, the emerging threat environment, characterized by a wide spectrum of actors that include near-peers, established nuclear powers, rogue nations, sub-national groups, and terrorist organizations that either now have access to nuclear weapons and ballistic missiles or may have such access over the next 15 years have combined to place the risk of EMP attack and adverse consequences on the US to a level that is not acceptable.

Current policy is to continue to provide EMP protection to strategic forces and their controls; however, the end of the Cold War has relaxed the discipline for achieving and maintaining that capability within these forces. The Department of Defense must continue to pursue the strategy for strategic systems to ensure that weapons delivery systems of the New Triad are EMP survivable, and that there is, at a minimum, a survivable “thin-line” of command and control capability to detect threats and direct the delivery systems. The Department of Defense has the capability to do this, and the costs can be within reasonable and practical limits.

The situation for general-purpose forces (GPF) is more complex. The success of these forces depends on the application of a superior force at times and places of our choosing. We accomplish this by using a relatively small force with enormous technological advantages due to superior information flow, advanced warfighting capabilities, and well-orchestrated joint combat operations. Our increasing dependence on advanced electronics systems results in the potential for an increased EMP vulnerability of our technologically advanced forces, and if unaddressed makes EMP employment by an adversary an attractive asymmetric option.

The United States must not permit an EMP attack to defeat its capability to prevail. The Commission believes it is not practical to protect all of the tactical forces of the US and its coalition partners from EMP in a regional conflict. A strategy of replacement and reinforcement will be necessary. However, there is a set of critical capabilities that is essential to tactical regional conflicts that must be available to these

reinforcements. This set includes satellite navigation systems, satellite and airborne intelligence and targeting systems, an adequate communications infrastructure, and missile defense.

The current capability to field a tactical force for regional conflict is inadequate in light of this requirement. Even though it has been US policy to create EMP-hardened tactical systems, the strategy for achieving this has been to use the DoD acquisition process. This has provided many equipment components that meet criteria for durability in an EMP environment, but this does not result in confidence that fielded forces, as a system, can reliably withstand EMP attack. Adherence to the equipment acquisition policy also has been spotty, and the huge challenge of organizing and fielding an EMP-durable tactical force has been a disincentive to applying the rigor and discipline needed to do so.

EMP durability should be provided to a selected set of tactical systems such that it will be practical to field tactical forces that cannot be neutralized by an EMP attack. The Department of Defense must perform a capabilities-based assessment of the most significant EMP threats to its tactical capabilities and develop strategies for coping with these threats in a reliable and effective manner.

Overall, little can be accomplished without the sustained attention and support of the leadership of the Department of Defense and Congress. This will require the personal involvement and cooperation among the Secretary of Defense, the Chairman of the Joint Chiefs, the Service Chiefs, and the appropriate congressional oversight committees in creating the necessary climate of concern; overseeing the development of strategy; and reaffirming the criticality of survivable and endurable military forces, including command, control, and communications (C3) in updated policy guidance, implementation directives, and instructions. Congressionally mandated annual reports from the Secretary of Defense and the Chairman of the Joint Chiefs on the status and progress for achieving EMP survivability of our fighting forces will emphasize the importance of the issue and help ensure that the necessary attention and support of the DoD leadership continues.

## APPENDIX A

### THE COMMISSION AND ITS METHOD

The Commission used a capability-based methodology to estimate potential EMP threats over the next 15 years.<sup>1</sup> The objective was to identify the range of plausible adversary EMP attack capabilities that cannot be excluded by prudent decision makers responsible for national and homeland security.

Bases for this assessment included current intelligence estimates of present and near-term military capabilities; current and past engineering accomplishments (what are adversaries likely to be capable of achieving, given accomplishments in other programs at comparable stages of development?); and trends impacting adversary military capabilities through 2018. In line with its capabilities-based approach, the Commission did not attempt to establish the relative likelihood of EMP strikes versus other forms of attack.

*...a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered looks strange; what looks strange is therefore improbable; what seems improbable need not be considered seriously.*

—Thomas C. Schelling, Foreword, in Roberta Wohlstetter, Pearl Harbor: Warning and Decision, Stanford University Press, 1962, p. vii.

Intelligence community organizations and the National Nuclear Security Administration's nuclear weapon laboratories (Lawrence Livermore, Los Alamos, and Sandia) provided excellent technical support to the Commission's analyses.<sup>2</sup> The Institute for Defense Analyses hosted and developed technical analyses for the Commission. While it benefited from these inputs, the Commission developed an independent assessment. Views expressed in this report are solely attributable to the Commission.

The Russian Federation (RF) has a sophisticated understanding of EMP that derives in part from the test era when the Soviet Union did high-altitude atmospheric tests

<sup>1</sup> Rob Mahoney, Capabilities-Based Methodology for Assessing Potential Adversary Capabilities, March 2004.

<sup>2</sup> The Commission's report and associated documents provide the necessarily classified assessments of future adversary capabilities for EMP attack and weapon issues.

over its own territory, impacting civilian infrastructures. To benefit from Russian expertise, the Commission:

- Sponsored research projects at Russian scientific institutions.
- Hosted a September 2003 US/Russian symposium on EMP at which presentations were given by Russian general officers.
- Sponsored a December 2003 technical seminar on EMP attended by scientists from the Russian Federation and the United States.

The Commission also reviewed additional relevant foreign research and programs and assessed foreign perspectives on EMP attacks.

In considering EMP, the Commission also gave attention to the coincident nuclear effects that would result from a detonation that produces EMP, e.g., possible disruption of the operations of, or damage to, satellites in space.

Different types of nuclear weapons produce different EMP effects. The Commission limited its attention to the most strategically significant cases in which detonation of one or few nuclear warheads could result in widespread, potentially long-duration disruption or damage that places at risk the functioning of American society or the effectiveness of US military forces.

In addition to examining potential threats, the Commission was charged to assess US vulnerabilities (civilian and military) to EMP and to recommend measures to counter EMP threats. For these purposes, the Commission reviewed research and best practices within the United States and other countries. Early in this review it became apparent that only limited EMP vulnerability testing had been accomplished for modern electronic systems and components. To partially remedy this deficit, the Commission sponsored illustrative testing; results are presented in the Commission's report.

Commissioners brought to this task a wide range of expertise, including service as an advisor to the President; senior management experience in both civilian and military agencies, national laboratories, and the corporate sector; and technical expertise in the design of nuclear weapons and in the hardening of systems against nuclear weapon effects.



## APPENDIX B

### COMMISSIONERS

*Dr. William R. Graham* is Chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. He is also Chairman of the Board and Chief Executive Officer of National Security Research Inc. (NSR), a Washington-based company that conducts technical, operational, and policy research and analysis related to US national security. In the recent past he has served as a member of several high-level study groups, including the Department of Defense Transformation Study Group, the Commission to Assess United States National Security Space Management and Organization (the Rumsfeld Commission on Space), and the Commission to Assess the Ballistic Missile Threat to the United States (also led by Hon. Donald Rumsfeld). From 1986–89 Dr. Graham was the director of the White House Office of Science and Technology Policy while he served concurrently as Science Advisor to President Reagan, Chairman of the Federal Joint Telecommunications Resources Board, and member of the Arms Control Experts Group. For 11 years he served as a member of the Board of Directors of the Watkins-Johnson Company.

*Dr. John S. Foster, Jr.*, is Chairman of the Board of GKN Aerospace Transparency Systems, chairman of Technology Strategies and Alliances, and consultant to Northrop Grumman Corporation, Sikorsky Aircraft Corp., Ninesigma, and Defense Group. He retired from TRW as Vice President, Science and Technology, in 1988 and continued to serve on the Board of Directors of TRW from 1988 to 1994. Dr. Foster was Director of Defense Research and Engineering for the Department of Defense from 1965–1973, serving under both Democratic and Republican administrations. In other distinguished service, Dr. Foster has been on the Air Force Scientific Advisory Board, the Army Scientific Advisory Panel, and the Ballistic Missile Defense Advisory Committee, Advanced Research Projects Agency. Until 1965, he was a panel consultant to the President's Science Advisory Committee, and from 1973–1990 he was a member of the President's Foreign Intelligence Advisory Board. He is a member of the Defense Science Board, which he chaired from January 1990–June 1993. From 1952–1962, Dr. Foster was with Lawrence Livermore National Laboratory (LLL), where he began as a Division Leader in experimental physics, became Associate Director in 1958, and became Director of LLL and Associate Director of the Lawrence Berkeley National Laboratory in 1961.

*Mr. Earl Gjeldre* is the Managing Director and Chief Executive Officer of Summit Group International, Ltd.; Summit Energy Group, Ltd.; Summit Energy International 2000, LLC; and Summit Power NW, LLC, primary participants in the development of over 5,000 megawatts of natural gas fired electric and wind generating plants within the United States. He has also held a number of government posts, serving as President George Herbert Walker Bush's Under (now called Deputy) Secretary and Chief Operating Officer of the US Department of the Interior (1989) and as President Ronald Reagan's Under Secretary and Chief Operating Officer of the US Department of the Interior (1985–1988). While in the Reagan administration he served concurrently as Special Envoy to China (1987), Deputy Chief of Mission for the US-Japan Science and Technology Treaty (1987–1988), and Counselor for Policy to the Director of the National Critical Materials Council (1986–1988); the Counselor to the Secretary and Chief Operating Officer of the US Department of Energy (1982-1985); and Deputy Administrator,

Chief Operating Officer, and Power Manager of the Bonneville Power Administration (1980-1982). Prior to 1980, he was a principal officer of the Bonneville Power Administration.

*Dr. Robert J. Hermann* is a senior partner of Global Technology Partners, LLC, a Boston-based investment firm that focuses on technology, defense aerospace, and related businesses worldwide. In 1998, Dr. Hermann retired from United Technologies Corporation, where he was Senior Vice President, Science and Technology. Prior to joining UTC in 1982, Dr. Hermann served 20 years with the National Security Agency with assignments in research and development, operations, and NATO. In 1977, he was appointed Principal Deputy Assistant Secretary of Defense for Communications, Command, Control, and Intelligence. In 1979, he was named Assistant Secretary of the Air Force for Research, Development, and Logistics and concurrently was Director of the National Reconnaissance Office.

*Mr. Henry (Hank) M. Kluepfel* is a Corporate Vice President for Corporate Development and Chief Scientist in the Enterprise Security Solutions Group of SAIC. He is the company's leading cyberspace security advisor to the President's National Security Telecommunications Advisory Committee (NSTAC) and the Network Reliability and Interoperability Council (NRIC). Mr. Kluepfel is widely recognized for his 30-plus years of experience in security technology research, design, tools, forensics, risk reduction, education, and awareness, and he is the author of industry's de facto standard security base guideline for the Signaling System Number 7 (SS7) networks connecting and controlling the world's public telecommunications networks. In past affiliations with Telcordia Technologies (formerly Bellcore), AT&T, BellSouth and Bell Labs, he led industry efforts to protect, detect, contain, and mitigate electronic and physical intrusions and led the industry's understanding of the need to balance technical, legal, and policy-based countermeasures to the then emerging hacker threat. He is recognized as a Certified Protection Professional by the American Society of Industrial Security and is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

*General (USAF, Ret.) Richard L. Lawson* is Chairman of Energy, Environment and Security Group, Ltd., and former President and CEO of the National Mining Association. He also serves as Vice Chairman of the Atlantic Council of the U.S; Chairman of the Energy Policy Committee of the US Energy Association; Chairman of the United States delegation to the World Mining Congress; and Chairman of the International Committee for Coal Research. Active duty positions included serving as Military Assistant to the President; Chief of Staff, Supreme Headquarters Allied Powers Europe; Director for Plans and Policy, Joint Chiefs of Staff; Deputy Director of Operations, Headquarters US Air Force; and Deputy Commander in Chief, US European Command.

*Dr. Gordon K. Soper* is Group Vice President of Defense Group Inc., responsible for broad direction of corporate goals relating to company support of government customers in areas of countering the proliferation of weapons of mass destruction, chemical/biological defense and domestic preparedness, treaty verification research, nuclear arms control and development of new business areas and growth of technical staff. He provides senior-level technical support on a range of task areas to the Defense Threat Reduction Agency (DTRA), the Chemical and Biological National Security Program of National Nuclear Security Administration, and the Counterproliferation and Chem/Bio Defense Office of the Office of the Secretary of Defense. Previously, Dr. Soper was Principal Deputy to the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Programs (ATSD (NCB); Director, Office of Strategic and Theater Nuclear Forces Command, Control and Communications (C3) of the Office of the

Assistant Secretary of Defense (C3I); and Associate Director for Engineering and Technology/Chief Scientist at the Defense Communications Agency.

*Dr. Lowell L. Wood, Jr.*, is a member of the Technical Advisory Group, US Senate Select Committee on Intelligence; a member of the Undersea Warfare Experts Group, US House of Representatives Committee on Armed Services; a visiting fellow at the Hoover Institution and Stanford University; and an officer and member of the Board of Directors of the Fannie and John Hertz Foundation. He is also a member of the Director's technical staff, University of California Lawrence Livermore National Laboratory, where he has held numerous positions since 1972.

*Dr. Joan Woodard* is Executive Vice President and Deputy Director of Sandia National Laboratories, responsible for all of Sandia's programs, operations, staff, and facilities. She is also responsible for the laboratory's strategic planning. Prior to her current appointment, Dr. Woodard was Vice President of the Energy, Information and Infrastructure Technology Division, where her responsibilities included energy-related projects in fossil energy, solar, wind, geothermal, geosciences, fusion, nuclear power safety and severe accident analysis, and medical isotope processing; environment-related programs in remediation, nuclear waste management and repository certification, and waste minimization; information technology programs in information surety, command and control systems, and distributed information systems; and programs responsible for security of the transportation of nuclear weapons and special nuclear materials, and safety of commercial aviation. Over 80% of the programs included industrial or academic partners, and the nature of the work ranged from basic research to prototype systems evaluation.



VOLUME I

# Assessing the Threat from Electromagnetic Pulse (EMP)

Executive Report

JULY 2017

Report of the Commission to Assess the Threat to the United States  
from Electromagnetic Pulse (EMP) Attack





# Assessing the Threat from Electromagnetic Pulse (EMP)

## Executive Report

**July 2017**

REPORT OF THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES  
FROM ELECTROMAGNETIC PULSE (EMP) ATTACK

---

The cover photo depicts Fishbowl Starfish Prime at 0 to 15 seconds from Maui Station in July 1962, courtesy of Los Alamos National Laboratory.

This report is a product of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. The Commission was established by Congress in the FY2001 National Defense Authorization Act, Title XIV, and was continued per the FY2016 National Defense Authorization Act, Section 1089.

The Commission completed its information-gathering in June 2017. The report was cleared for open publication by the DoD Office of Prepublication and Security Review on April 9, 2018.

This report is unclassified and cleared for public release.

TABLE OF CONTENTS

---

EXECUTIVE SUMMARY ..... 1

OBSERVATIONS, ANALYSIS, AND RECOMMENDATIONS ..... 4

    The EMP Threat ..... 4

    Barriers to Effective Protection from EMP ..... 6

    Late-Time EMP Fields and Effects (E3) ..... 13

    Testing Selected EMP-vulnerable Full-system Equipment to Failure..... 15

    Intelligence Community Assessment of the EMP Threat..... 16

CONCLUSIONS ..... 17

APPENDIX A   Legislation Re-establishing the Commission..... 19

APPENDIX B   High Altitude Nuclear Explosion-Generated Electromagnetic Effects..... 20

BIOGRAPHIES..... 22

    Commissioners..... 22

    Senior Advisors..... 24

COMMISSION REPORTS ..... 27

## ACRONYMS AND ABBREVIATIONS

---

DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
ELECTRA	Electromagnetic Effects Comparison Test and Reliability Assessment
EMP	electromagnetic pulse
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
FERC	Federal Energy Regulatory Commission
HEMP	high-altitude electromagnetic pulse
NERC	North American Electric Reliability Corporation
NRC	Nuclear Regulatory Commission

## PREFACE

---

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (herein and elsewhere referred to as “the EMP Commission”) was re-established by the National Defense Authorization Act (NDAA) for Fiscal Year 2016 on November 25, 2015, and funded by the appropriation for the Commission on December 18, 2015. Delays by the Department of Defense in providing funding, clearance support, and contractor support to the Commission throughout 2016 delayed the first meeting until January 2017. The Commission’s statutory mandate terminated at the end of June 2017 in accord with the terms of the NDAA. EMP is a complex subject, and the DoD provided only limited support beyond this time to allow the Commission to complete its work even though funding to continue was available. As a result, the Commission could not adequately complete the full scope of the Congressional charge as described in Appendix A. This report is therefore necessarily limited, yet the Commission is confident this material contained herein is accurate and trusts it is valuable to the recipients.

Following the last meeting of the EMP Commission on June 8-9, 2017, global events have strengthened public awareness of the worldwide vulnerability of critical infrastructures to high altitude EMP. North Korean state news, KCNA, displayed photos of an alleged thermonuclear weapon and claimed on September 3, 2017, “The H-bomb, the explosive power of which is adjustable from tens of kilotons to hundreds of kilotons, is a multi-functional thermonuclear nuke [sic] with great destructive power which can be detonated even at high altitudes for super-powerful EMP (electromagnetic pulse) attack according to strategic goals.” The United States, its territories, and allies are therefore the target of current threats by the government of North Korea that specifically include EMP, and also include further development and exploitation of high altitude EMP weapons.

## EXECUTIVE SUMMARY

---

The critical national infrastructure in the United States faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, as well as from natural EMP from a solar superstorm. During the Cold War, the U.S. was primarily concerned about an EMP attack generated by a high-altitude nuclear weapon as a tactic by which the Soviet Union could suppress the U.S. national command authority and the ability to respond to a nuclear attack—and thus negate the deterrence value of assured nuclear retaliation. Within the last decade, newly-armed adversaries, including North Korea, have been developing the ability and threatening to carry out an EMP attack against the United States. Such an attack would give countries that have only a small number of nuclear weapons the ability to cause widespread, long-lasting damage to critical national infrastructures, to the United States itself as a viable country, and to the survival of a majority of its population.

Major efforts have been undertaken by the Department of Defense to assure that the U.S. national command authority and U.S. strategic forces could survive and operate after an EMP attack. However, no major efforts were thought necessary to protect critical national infrastructures, relying on nuclear deterrence to protect them. With the development of small nuclear arsenals and long-range missiles by small, hostile, and potentially irrational adversaries, including North Korea, the threat of a nuclear EMP attack against the U.S. becomes one of the few ways that such a country could inflict devastating damage to the United States. It is critical, therefore, that the U.S. national leadership address the EMP threat as a critical and existential issue, and give a high priority to assuring the leadership is engaged and the necessary steps are taken to protect the country from EMP. Otherwise, foreign adversaries may reasonably consider such an attack as one which can gravely damage the U.S. by striking at its technological Achilles' heel without having to engage the U.S. military.

Protecting and defending the national electric grid and other critical infrastructures from cyber and EMP could be accomplished at reasonable cost and minimal disruption to the present systems that comprise U.S. critical infrastructure. This is commensurate with Trump Administration plans to repair and improve U.S. infrastructures, increase their reliability, and strengthen homeland defense and military capability. Continued failure to address the U.S. vulnerability to EMP generated by a high-altitude nuclear weapon invites such an attack.

The single most important action *that requires immediate action* to advance U.S. security and survivability is that the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat (*Recommendation 1*). Current institutional authorities and responsibilities—government, industry, regulatory agencies—are fragmented, incomplete,



under-resourced, and unable to protect and defend against foreign hostile EMP threats or solar superstorms.

The Commission highly commends President Trump's Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, signed on May 11, 2017. **The Commission strongly recommends that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection** (*Recommendation 2*), because all-out cyber warfare may well include nuclear EMP attack. Protecting against nuclear EMP will also protect against natural EMP from solar storms, although the converse is not true. The United States must take steps to mitigate its current state of vulnerability to these well-known natural and adversary EMP threats. To further this endeavor, **the Commission encourages the President to work with Congressional leaders to establish a joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership to achieve, on an accelerated basis, the protection of critical national infrastructures.** (*Recommendation 3*).

Across the U.S. government, the DoD and its supporting laboratories and contractors have by far the most knowledge, data, and experience related to the production of and survival from nuclear weapon-generated EMP. However, the DoD has largely failed to make this knowledge available to other government agencies and to the organizations that develop, build, and operate U.S. critical national infrastructure. For example, there has been a continuing unwillingness of the DoD to provide specific information about the EMP environment to the commercial community owing to classification restrictions. Today the DHS looks to the DOE to provide guidance and direction for protecting the national electric power grids. Such a course of action would take longer and cost more compared to establishing a program of cooperation with the knowledgeable parts of the DoD.

In the absence of an unclassified, well-informed U.S. late-time (E3) EMP threat specification [described in Appendix B], electric utilities, electrical equipment manufacturers, and electric research institutes have articulated their inability to design appropriate countermeasures and to justify cost recovery for capital investments programs. Accordingly, this Commission has prioritized the development of late-time E3 threat specifications, derived from openly available test data. As part of this assessment, Commission staff analyzed E3 EMP measurements from two nuclear high-altitude tests performed by the Soviet Union in 1962. Physicists with extensive experience in EMP modeling used these data waveforms and an understanding of the scaling relationships for the nuclear explosion-induced upper atmospheric heave phenomenon that produces the E3 EMP electromagnetic fields by disturbing the natural magnetic field of the Earth. Based on this analysis, **the Commission recommends that government agencies and industries adopt new standards to protect critical national infrastructures from damaging E3 EMP heave fields, with more realistic standards of 85 V/km** (*Recommendation 4*). Typical waveforms for commercial applications are included in Appendix B that should prove useful for the protection of the national power grids. **The Commission also recommends**

**electric grid equipment with long-replacement times such as large power transformers be tested to system failure** (*Recommendation 5*).

In the area of national intelligence, the Commission found that the classified report by the Joint Atomic Energy Intelligence Committee (JAEIC) on EMP issued in 2014 is factually erroneous and analytically unsound. **The Commission recommends the Director of National Intelligence circulate to all recipients of the 2014 JAEIC report the EMP Commission critique of that report and direct a new assessment be prepared that supersedes the 2014 JAEIC EMP report** (*Recommendation 6*). The new report should be reviewed by experts in the subject areas being addressed and circulated to all the recipients of the 2014 assessment.

## OBSERVATIONS, ANALYSIS, AND RECOMMENDATIONS

---

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack was previously convened by the Congress from 2001-2005 and from 2007-2008, and currently from 2016-2017.<sup>1,2</sup>

The current Commission assessment is consistent with the previous recommendations. In summary, the Commission sees the high-altitude nuclear explosion-generated electromagnetic pulse as an existential threat to the survival of the United States and its allies that can be exploited by major nuclear powers and small-scale nuclear weapon powers, including North Korea and non-state actors, such as nuclear-armed terrorists.

### THE EMP THREAT

The United States—and modern civilization more generally—faces a present and continuing existential threat from naturally occurring and manmade electromagnetic pulse assault and related attacks on military and critical national infrastructures. A nationwide blackout of the electric power grid and grid-dependent critical infrastructures—communications, transportation, sanitation, food and water supply—could plausibly last a year or longer.<sup>3</sup> Many of the systems designed to provide renewable, stand-alone power in case of an emergency, such as generators, uninterruptable power supplies (UPS), and renewable energy grid components, are also vulnerable to EMP attack.<sup>4</sup>

A long-term outage owing to EMP could disable most critical supply chains, leaving the U.S. population living in conditions similar to centuries past, prior to the advent of electric power.<sup>5</sup> In the 1800s, the U.S. population was less than 60 million, and those people had many skills and assets necessary for survival without today's infrastructure. An extended blackout today could result in the death of a large fraction of the American people through the effects of societal collapse, disease, and starvation. While national planning and preparation for such events could help mitigate the damage, few such actions are currently underway or even being contemplated.

---

<sup>1</sup> The EMP Commission has previously published two unclassified reports: *Executive Report* dated 2004, and *Critical National Infrastructures*, dated 2008.

<sup>2</sup> See Appendix A, "Legislation Re-establishing the Commission," National Defense Authorization Act for Fiscal Year 2016, Sec. 1089.

<sup>3</sup> For example, see E. Conrad, G. Gurtman, G. Kweder, M. Mandell, and W. White. *Collateral Damage to Satellites from an EMP Attack*, Report to the EMP Commission, DTRA-IR-10.22.

<sup>4</sup> Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *HEMP Direct Drive Testing of Sample Solar Systems. Report of the EMP Commission*. July 2017.

<sup>5</sup> National Security Telecommunications Advisory Committee (NSTAC). *People and Processes: Current State of Telecommunications and Electric Power*, January 31, 2006.

Combined-arms cyber warfare, as described in the military doctrines of Russia, China, North Korea, and Iran, may use combinations of cyber-, sabotage-, and ultimately nuclear EMP-attack to impair the United States quickly and decisively by blacking-out large portions of its electric grid and other critical infrastructures.<sup>6</sup> Foreign adversaries may aptly consider nuclear EMP attack a weapon that can gravely damage the U.S. by striking at its technological Achilles Heel, without having to confront the U.S. military. The synergism of such combined arms is described in the military doctrines of all these potential adversaries as the greatest revolution in military affairs in history—one which projects rendering obsolete many, if not all, traditional instruments of military power.

Any of several threats, as described here, must be considered:

- Solar superstorms can generate natural EMP over remarkably wide areas. Recurrence of the Carrington Event of 1859 is considered by many to be inevitable.<sup>7</sup> NASA estimates the likelihood of such an event to be 10 to 12 percent per decade, making it very likely that Earth will be affected by a solar superstorm within a matter of decades.<sup>8</sup> Such an event could blackout electric grids and other life-sustaining critical infrastructures, putting at risk the lives of many millions.
- Nuclear EMP attack might be conducted with only a single nuclear weapon detonated at high altitude or a few weapons at several hundred kilometers. These could be delivered by satellite, by a wide variety of long- and short-range missiles, including cruise and anti-ship missiles, by a jet doing a zoom-climb, or even by a high-altitude balloon. Some modes of attack could be executed relatively anonymously, thereby impairing deterrence.
- Russia, China, and North Korea now have the capability to conduct a nuclear EMP attack against the U.S. All have practiced or described contingency plans to do so.<sup>9</sup> Terrorists or other less-sophisticated actors also might mount a nuclear EMP attack if

---

<sup>6</sup> For example, see Army of the Islamic Republic of Iran, *Passive Defense: Approach to the Threat Center* (Tehran: Martyr Lt. General Sayad Shirazi Center for Education and Research, Spring 2010); Shen Weiguang, *World War, the Third World War—Total Information Warfare*; General Vladimir Slipchenko, *Non-Contact Wars* (Moscow: January 1, 2000) translated in FBIS CEP20001213000001; and comments on North Korean state news on 3 September 2017.

<sup>7</sup> R.A. Lovett. "What if the biggest solar storm on record happened today?" *National Geographic News*, March 4, 2011.

<sup>8</sup> P. Riley and J.J. Love, "Extreme geomagnetic storms: Probabilistic forecasts and their uncertainties," *Space Weather*, v. 15, Jan. 2017, pp. 53-64. The probability of an extreme geomagnetic storm on the scale of the Carrington event varies based on the type of distribution used in the analysis from 3 (lognormal) to 10 (power law) per decade; see also P. Riley, "On the probability of occurrence of extreme space weather," *Space Weather*, v. 10, Feb. 2012, pp. 2101-2114, which estimates 12 percent per decade.

<sup>9</sup> For example, see Army of the Islamic Republic of Iran, *Passive Defense: Approach to the Threat Center* (Tehran: Martyr Lt. General Sayad Shirazi Center for Education and Research, Spring 2010); Shen Weiguang, *World War, the Third World War—Total Information Warfare*; General Vladimir Slipchenko, *Non-Contact Wars* (Moscow: January 1, 2000) translated in FBIS CEP20001213000001; and comments on North Korean state news on 3 September 2017.

they have access to a suitable nuclear explosive. For missile delivery, no re-entry system or accurate missile guidance would be necessary.

- Cyber-attack, using computer viruses and related means, might be able to blackout much of the national electric grid for extended intervals. According to U.S. Cyber Command, Russia and China currently have such capability and it may only be a matter of time before other adversaries also gain a similar capability.<sup>10</sup>
- The U.S. electrical grid could be sabotaged by damaging extra-high-voltage (EHV) transformers using rifles, explosives, or non-nuclear EMP or directed energy weapons. Attacking less than a dozen key substations could result in protracted and widespread blackouts, according to the public statements of a past Chairman of the U.S. Federal Energy Regulatory Commission (FERC).<sup>11</sup> At least one substantive rehearsal of such an attack may have already taken place, at the Metcalf substation in the San Francisco Bay area.<sup>12</sup>
- The Commission highly commends President Trump's Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" signed on May 11, 2017. Including the potential for EMP as part of a cyber-attack is prudent when the current vulnerability of the U.S. electrical grid and critical infrastructures is taken into account.

***Recommendation 2:** The Commission strongly recommends that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection.*

## BARRIERS TO EFFECTIVE PROTECTION FROM EMP

The government's response to the EMP Commission recommendations made in 2008 is not encouraging.

In a 2011 study, the DoD's JASON advisory panel concluded that the federal response to the EMP risk "is poorly organized; no one is in charge, resulting in duplications and omissions between agencies."<sup>13</sup>

---

<sup>10</sup> Admiral Michael Rogers, Director, National Security Agency and Commander, U.S. Cyber Command. "Cybersecurity Threats: The Way Forward," Testimony, House Permanent Select Committee on Intelligence, Nov. 20, 2014.

<sup>11</sup> R. Smith. "U.S. Risks National Blackout From Small-Scale Attack," Wall Street Journal, March 12, 2014; and R. Smith. "How America Could Go Dark," Wall Street Journal, July 14, 2016.

<sup>12</sup> R. Smith. "Assault On California Power Station Raises Alarm On Potential For Terrorism," Wall Street Journal, February 5, 2014.

<sup>13</sup> MITRE, 2011. Impacts of Severe Space Weather on the Electric Grid, MITRE, 2011, Report JSR-11-320.

A survey of recent government reports that address the protection of critical infrastructure reveals that none mention EMP, although critical infrastructure risks, resilience, protection, and availability are central to each report and to each Departments' mission.<sup>14</sup>

During a hearing before the Senate Homeland Security and Government Affairs (SHSGA) Committee on July 22, 2015, the U.S. Government Accountability Office (GAO) acknowledged that none of the recommendations of the EMP Commission to protect the national grid from EMP have been implemented by DHS, DOE, U.S. FERC or the North American Electric Reliability Corporation (NERC).<sup>15</sup> The GAO report explained lack of progress in protecting the national electric grid from EMP as due to a lack of leadership, because no one was in charge of solving the EMP problem, as follows: "DHS and DOE, in conjunction with industry, have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks."<sup>16</sup>

In March 2016, GAO reported that none of the essential measures recommended by the EMP Commission to protect the national electric grid had been addressed by Federal agencies, as shown in Table 1. The report stated that agencies had primarily drafted industry standards and federal guidelines and have only completed related research reports rather than implementing the resulting recommendations.<sup>17</sup>

**Table 1: Status of Previous Recommendations from the EMP Commission**

<i>Recommendation</i>	<i>Action</i>
Expand and extend emergency power supplies	None
Extend black start capability	None
Prioritize and protect critical nodes	None
Expand and assure intelligent islanding capability	None
Assure protection of high-value generation assets	None
Assure protection of high-value transmission assets	None
Assure sufficient numbers of adequately trained recovery personnel	None

Some efforts have been made, but these have been frustrated by a lack of leadership. For example, in October 2016, President Obama issued a comprehensive Executive Order for

<sup>14</sup> These reports include *Mitigation of Power Outage Risks for Department of Defense Facilities and Activities 2015*, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (DHS), and *U.S. Department of Energy Strategic Plan 2014-2018*.

<sup>15</sup> The Nuclear Regulatory Commission could be added to the list of deficient government agencies in that it has failed to similarly protect the nuclear power reactors and spent fuel storage facilities for which they are responsible.

<sup>16</sup> U.S. Senate Committee on Homeland Security and Governmental Affairs. Full committee hearing on "Protecting the Electric Grid from the Potential Threats of Solar Storms and Electromagnetic Pulse," held July 22, 2015.

<sup>17</sup> Government Accountability Office. *Critical Infrastructure Protection: Federal Agencies Have Taken Actions To Address Electromagnetic Risks, But Opportunities Exist To Further Assess Risks And Strengthen Collaboration*, GAO-16-243, March 2016.



coordinating efforts to prepare the nation for space weather events.<sup>18</sup> The primary federal mechanism for coordination is the interagency Space Weather Operations, Research, and Mitigation (SWORM) task force. This Executive Order gave DHS overall leadership in geomagnetic disturbance preparedness and the DOE leadership in addressing grid impacts, yet neither department has yet done a credible job of preparing the U.S. for such storms. This minimal effort did not address preparing the nation for similar wide-area effects on the electric power grid caused by an EMP attack.

Despite advocacy for a combined standard to protect the U.S. bulk power system from both man-made EMP and natural occurring solar storms, FERC in May 2013 ordered development of operating procedures and hardware protection standards only for solar geomagnetic disturbances.<sup>19</sup> Upon recommendations of the designated Electric Reliability Organization, NERC, FERC issued guidance for operational procedures to cope with solar storms in FERC Order 779.<sup>20</sup> These procedures excluded owner-operator requirements to protect generating facilities with generator step-up transformers, even those that have experienced transformer fires and explosions in prior solar storms. After development of a benchmark model by a NERC Geomagnetic Disturbance Task Force, in September 2016 FERC issued a standard for phased assessments of potential hardware protections that utilities would perform over a period of years, but without any mandatory hardware-protection installations actually required.<sup>21</sup>

These scattered, incoherent, and inadequate responses are a clear indication that for at least the last decade, critical national infrastructure protection from EMP has been largely ignored or dismissed by major departments of the U.S. government. The unaddressed vulnerability of the U.S. to EMP is an incentive for hostile powers to attack or, at a minimum, to develop capabilities for HEMP attack.

### *Interagency Cooperation and Centralized Governance*

The DoD has, since 1962, understood the data, phenomena, magnitude, and importance of high-altitude electromagnetic pulse (HEMP) effects, and has applied that knowledge to certain military systems.<sup>22</sup> However, DoD has not adequately transferred that knowledge to other agencies of the government and to organizations that provide critical national infrastructures, such as electrical power and communications utilities. This is surprising because

---

<sup>18</sup> The White House. "Coordinating Efforts to Prepare the Nation for Space Weather Events," Executive Order 13744, October 13, 2016.

<sup>19</sup> FERC Order No. 779, Reliability Standards for Geomagnetic Disturbances, May 16, 2013.

<sup>20</sup> FERC Order No. 797, Reliability Standard for Geomagnetic Disturbance Operations, June 19, 2014.

<sup>21</sup> FERC Order No. 830, Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events, September 22, 2016. On the last full day of the Obama Administration, FERC denied four appeals for rehearing of Order 830, in FERC Order No. 830-A, January 19, 2017.

<sup>22</sup> Operation Fishbowl in 1962 was the last high-altitude nuclear test series conducted by the U.S. military.

the DoD depends upon these same critical national infrastructures for domestic military operations as well as the security of the nation. To the contrary, the DoD has withheld public distribution of and has classified much of the data and technology that underlies protection against EMP even though potential adversaries of the U.S. are generally familiar with such technology. It is interesting to note that some of the most useful data available for predicting the electromagnetic fields produced by a nuclear explosion have been derived from data published by the former Soviet Union.<sup>23</sup>

In the absence of technology transfer and other support by the DoD to other agencies of the government and the industries supporting critical national infrastructures, the DHS depends upon the DOE, as their Sector-Specific Agency, to provide guidance and direction for protecting the national electric power grids.<sup>24</sup> The DOE relies on the National Laboratories under its sponsorship to provide such guidance and direction. While it is possible to conduct new testing and analysis required to generate the data, such a course of action would take longer and cost more compared to establishing a program of cooperation with the knowledgeable offices and laboratories in the DoD. A more efficient alternative is establishing a DoD policy that makes much of the defense-controlled data concerning EMP technology available to the government agencies and industry that support the U.S. critical national electric power infrastructure.

### *Regulatory Conflicts of Interest*

The current institutional arrangements for protecting and improving the reliability of the electric grids and other critical infrastructures through the FERC and the NERC are not designed to address major national security threats to the electric power grids and other national critical infrastructures. Using FERC and NERC to achieve this level of national security has proven to be ineffectual. New institutional arrangements are needed to advance preparedness to guard against EMP and related threats to our critical national infrastructures.

The current U.S. power industry is largely self-regulated under FERC, NERC, Nuclear Regulatory Commission (NRC), and the electric power industry companies. The EMP Commission assesses that the existing regulatory framework for safeguarding the security and reliability of the electric power grid, which is based upon a partnership between the U.S. Government's FERC and the private non-profit NERC representing the utilities, is not set up to protect the U.S. against hostile EMP attack. For example, the standards for protecting the power grids from geomagnetic disturbances caused by solar storms prescribe threat levels

---

<sup>23</sup> One of the best references for understanding and protecting against EMP is a translation of a Soviet handbook, entitled, "The Physics of Nuclear Explosions," Ministry of Defense of the Russian Federation, Central Institute of Physics and Technology, Volumes 1 and 2, ISBN 5-02-015124-6, 1997.

<sup>24</sup> See the DHS Energy Sector overview at <https://www.dhs.gov/energy-sector>

below those recorded during major storms of historical record.<sup>25</sup> In May 2013, FERC ordered entities in the bulk power system to develop reliability standards to protect against solar geomagnetic disturbances (GMD). Generator operators were excluded. Despite multiple requests for FERC to develop a joint reliability standard for grid protection from both EMP and GMD hazards, NERC has only proposed limited standards for solar storm protection.<sup>26,27</sup> This can be attributed to the industry's desire to minimize protection requirements.

In public testimony before Congress, FERC has stated that it lacks regulatory power to compel NERC and the electric power industry to protect the grid from natural and nuclear EMP and other threats.<sup>28</sup> Consider the contrast in regulatory authority of the U.S. Federal Energy Regulatory Commission and similar regulatory agencies in the U.S. Government:

- The NRC has regulatory power to compel the nuclear power industry to incorporate nuclear reactor design features to make nuclear power safe. (To date, however, the NRC has not incorporated EMP survival criteria into design regulations. Further, that Commission has not required that spare transformers or emergency diesel generators be certified to be EMP-protected.)
- The U.S. Federal Aviation Administration (FAA) has regulatory power to compel the airline industry to ground aircraft considered unsafe, to change aircraft operating procedures considered unsafe, and to make repairs or improvements to aircraft in order to protect the lives of airline passengers.
- The U.S. Department of Transportation (DOT) has regulatory power to compel the automobile industry to install on cars safety glass, seatbelts, and airbags in order to protect the lives of the driving public.
- The U.S. Food and Drug Administration (FDA) has power to regulate the quality of food and drugs, and can ban under criminal penalty the sale of products deemed by the FDA to be unsafe to the public.
- The U.S. Environmental Protection Agency (EPA) has power to regulate clean air, clean water, and hazardous materials deemed by the EPA to be unsafe to the public.

---

<sup>25</sup> J.G. Kappenman and W. Radasky, *Examination of NERC GMD Standards and Validation of Ground Models and Geo-Electric Fields, Report to the EMP Commission*, July 28, 2017. See also Foundation for Resilient Societies, Comments Submitted on Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events, FERC Docket No. RM15-11-000, July 27, 2015; supplementary comments submitted August 10, 2015.

<sup>26</sup> Requests for rehearing of Order No. 830 were filed by the Foundation for Resilient Societies, Edison Electric Institute, Center for Security Policy, and Jewish Institute for National Security Affairs. These were denied in Docket No. RM15-11-001, issued January 19, 2017.

<sup>27</sup> U.S. Federal Energy Regulatory Commission. "Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events," Docket No. RM15-11-000; Order No. 830, issued January 21, 2016.

<sup>28</sup> Testimony of Joseph McClelland, U.S. FERC's Director of the Office of Electric Reliability, before the Senate Committee on Energy and Natural Resources (July 17, 2012); T. Sanders, "FERC's McClelland Calls For Enhanced Authority On Cyber-Security" Washington Energy Report, July 20, 2012.

Unlike the NRC, FAA, DOT, FDA, EPA, and most other U.S. government regulatory agencies, FERC does not have legal authority to compel the industry it is charged to regulate to act in the public interest. The U.S. FERC even lacks legal power to direct the electric utilities to install devices to protect the grid.

Currently, U.S. FERC only has the power to require NERC to propose a standard to protect the grid. NERC Standards are approved, or rejected, or remanded for further consideration by its membership, which is largely made up of representatives from the electric power industry. Once NERC proposes a standard to FERC, FERC cannot modify the standard, but must either accept or reject the proposed standard. If FERC rejects the proposed standard, NERC goes back to the drawing board, and the process starts all over again, often resulting in long delays for implementation of standards.

The DOE Quadrennial Energy Review released in January 2017 recommended, "... in the area of cybersecurity, Congress should provide FERC with authority to modify NERC-proposed reliability standards—or to promulgate new standards directly—if it finds that expeditious action is needed to protect national security in the face of fast-developing new threats to the grid. This narrow expansion of FERC's authority would complement DOE's national security authorities related to grid-security emergencies affecting critical electric infrastructure and defense-critical electricity infrastructure..."<sup>29</sup>

It is notable that this proposal would limit additional FERC authority to strengthen a reliability standard or to promulgate a new standard "in the area of cybersecurity." Although EMP hazards were not explicitly included in the proposed supplemental FERC authorities, EMP could be included under the cyber threat rubric as it directly debilitates cyber electronic systems.

Moreover, testifying before a House Energy and Commerce Subcommittee on February 1, 2017, the Chief Executive Officer of NERC expressed opposition to any Congressional grant of new FERC legislative authority to strengthen or directly promulgate any new grid reliability standard that NERC had not already proposed, thereby undermining the FERC's ability to protect the U.S. electric power grids from EMP attack.<sup>30</sup>

The geomagnetic disturbance standards proposed by the NERC, which the FERC has adopted to date, substantially underestimate the magnitude of historical and future geomagnetic disturbances. No standards for protecting the grid against nuclear or non-nuclear EMP weapons have been proposed or adopted.<sup>31</sup>

---

<sup>29</sup> U.S. Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the QER*, January 2017, pp. S-16 and 7-7.

<sup>30</sup> G.W. Cauley, *Hearing on the Electricity Sector's Efforts to Respond to Cybersecurity Threats*, Testimony before the House Subcommittee on Energy, Energy and Commerce Committee, February 1, 2017.

<sup>31</sup> Federal Energy Regulatory Commission (FERC) Order 779, *Final Rule on Reliability Standard for Geomagnetic Disturbances*, Reliability Standard EOP-010-1, June 25, 2014; FERC Order 830, *Transmission System Planned*

### *Recommendations to Improve Governance*

The Commission's chief recommendation is made to address the critical leadership deficiency.

***Recommendation 1:*** *The Commission recommends the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat.*

The 2017 Presidential initiative to repair and strengthen U.S. infrastructure, cyber security, homeland defense, and military capability presents a unique opportunity to include measures for EMP protection that could obviate the existential threats from solar superstorms and combined-arms cyber warfare.

A second recommendation in the area of governance is to ensure a whole-of-government approach to the challenge of EMP protection. A joint Presidential-Congressional Commission on critical infrastructure protection could engage the free world's preeminent experts on EMP and related threats to serve the interagency in a manner akin to other advisory Commissions. For example, between 1947 and 1974, the Atomic Energy Commission advised the administration on how to attain most quickly and most cost-effectively the protection essential to long-term national survival and well-being. Such a structure would help the U.S. move beyond the current state of vulnerability to well-understood natural and man-made EMP threats.

***Recommendation 3:*** *The Commission encourages the President to work with Congressional leaders to establish a joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership to achieve, on an accelerated basis, the protection of critical national infrastructures.*

Protecting the national electric grid and other critical infrastructures from the most severe of these threats—nuclear EMP attack—could be done in ways that protect against or significantly mitigate some other threats. Extensively tested, performance-proven technologies for EMP hardening have been developed and used by the DoD to protect critical military systems for over 50 years, and can be affordably adapted to protect electric grids and other critical infrastructures, at low-cost relative to that of an EMP catastrophe.

For example, the EMP Commission estimated in its 2008 report, critical parts of the national electric grid could be protected for about \$2 billion.

---

*Performance for Geomagnetic Disturbance Events, Reliability Standard TPL-007-1, Sep. 22, 2016, and FERC Order 830-A, Denying Rehearing (of Order 830), January 19, 2017.*

The U.S. knowledge base on EMP threat levels and waveforms is adequate. Likewise, EMP protection engineering is mature such that system protection programs can proceed immediately, without the need for lengthy additional research. The Commission is concerned that DOE and the Electric Power Research Institute (EPRI) are pursuing lengthy research and development programs to redefine environments and determine EMP system effects that introduce unnecessary delays in actual implementation of grid protection. The Commission finds that diverting these resources to pilot demonstration programs to protect selected sectors of the electric power grid would better serve the intent to protect the U.S. electrical grid. A strategic plan, along with the leadership to implement it, is needed now.

### LATE-TIME EMP FIELDS AND EFFECTS (E3)

Solar superstorms, more formally called coronal mass ejection events, produce fields similar to EMP E3 effects. A NASA analysis states that “historical aurora records suggest a return period of 50 years for Québec-level storms and 150 years for very extreme storms, such as the 1859 Carrington event.”<sup>32</sup> A high-altitude nuclear EMP event would also include higher frequency E1 and E2 fields. An understanding of the range of fields produced is required to understand their effects and the threat to the electrical grid.

To study the impact of these types of electromagnetic fields on extended electrical and communications transmission lines associated with the critical infrastructures, utilities need upper-bound, open-source information for the late-time (E3) high-altitude electromagnetic pulse threat waveform and its ground pattern. This need arises because of the effect of very low frequency electric field component (E3) coupled to horizontal electrical conductors, such as power transmission lines, that induce large quasi-direct current in those lines. When the quasi-direct current travels through the windings of large transformers handling high levels of power, they shift the magnetic field operating point in the core of the transformers, causing the transformer to generate abnormal harmonic waveforms that neither the transformer nor the electrical power system are able to manage. This results in overheating and damage to the transformers. Therefore, it is important that an unclassified bounding-case E3 waveform be available to those working in the commercial power equipment development and operation sectors.

While the DoD has developed high-altitude EMP waveforms (E1, E2, and E3) for its purposes, these are classified and not available for commercial use. The DoD policy of keeping its E3 threat specifications classified, and therefore not available to designers and operators of the U.S. national power grids, is, in the view of the Commission, much more damaging to the protection of U.S. critical national electrical power infrastructure than its release would be helpful to U.S. adversaries. Some potential adversaries, including Russia, have collected some of the

---

<sup>32</sup> T. Phillips. “Near Miss: The Solar Superstorm of July 2012.” Science@NASA, July 23, 2014



best E3 data during their high altitude nuclear tests and therefore are already aware of the magnitude of the E3 fields. The withholding of E3 information is a DoD policy that is neither in the interest of U.S. national security and survival, nor in the interest of the DoD, because the DoD depends on commercial power for many of its activities.

In the absence of an unclassified, well-informed E3 specification, the Commission tasked experts to assess the openly available E3 HEMP measurements from two nuclear high-altitude tests performed by the Soviet Union in 1962. Using these data and an understanding of the scaling relationships for the E3 HEMP heave phenomenon, bounding waveforms for commercial applications were developed.

Because the measured quantities during these tests were the magnetic fields, it is possible for technologists familiar with electromagnetic theory to compute the E3 electric fields, using known ground conductivity profiles. Other ground conductivity profiles could lead to even higher fields, but some of these profiles do not cover a very large area of the Earth.

After computing the electric fields using the Soviet measurements, the results were scaled to account for the fact that the Soviet measurement locations were not at the optimum points on the ground to capture the maximum peak fields. This process determined that the scaled maximum peak E3 EMP heave field would have been 66 volts per kilometer (V/km) for the magnetic latitude of the Soviet tests.

The measured results were also evaluated for the E3 EMP heave field. This parameter increases for burst points closer to the geomagnetic equator, displaying inverse latitude behavior compared to solar GMD fields. This scaling increases the maximum peak electric field up to 85 V/km for locations in the southern continental United States, and 102 V/km for locations near the geomagnetic equator, such as Hawaii. The levels in Alaska would be lower, with a peak value of 38 V/km. While as noted these are not worst-case levels, they are reasonable upper-bound values useful in designing, evaluating, and operating bulk electrical power transmission systems and long-haul copper and fiber communication and data networks.<sup>33</sup>

***Recommendation 4:** The Commission recommends that government agencies and industries adopt new standards to protect critical national infrastructures from damaging E3 EMP heave fields, with more realistic standards of 85 V/km.*

Typical waveforms for commercial applications are included in Appendix B that should prove useful for the protection of the national power grids.

---

<sup>33</sup> Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures. Report of the EMP Commission*, July 2017.

## TESTING SELECTED EMP-VULNERABLE FULL-SYSTEM EQUIPMENT TO FAILURE

Some equipment that is essential for operation of critical infrastructures may be more economically stockpiled and stored in EMP-shielded structures than redesigned to be EMP-hardened. Other equipment with long replacement times or uncertainty of availability after an EMP attack will require EMP-hardening against E1, E2 and E3 hazards. While modeling of EMP vulnerability and mitigation measures is desirable, there is no substitute for full system testing to failure to project the likely post-EMP attack operability or prompt recovery of critical infrastructure equipment.

The Defense Nuclear Agency and its successor Defense Special Weapons Agency sponsored an innovative EMP evaluation program called the Electromagnetic Effects Comparison Test and Reliability Assessment (ELECTRA) from 1992 to 1995. ELECTRA performed both pre-test expert assessments of EMP survivability and system tests to failure using actual threat-level illumination and current injection testing. The ELECTRA Technical Review Group compared sealed-envelope analytical predictions of system EMP effects against post-test system effects.<sup>34</sup> Key findings from ELECTRA are pertinent to development of reliable and cost-effective EMP equipment protection and recovery programs.

The ELECTRA forecasting and test assessment program demonstrated that EMP system effects were most pronounced for modern electronic systems having unprotected external power and signal lines.<sup>35</sup> Moreover, forecasts by EMP survivability experts of pass-fail testing outcomes were no better than random coin-tossing when assessing actual system failures. Predictions of whether or not EMP effects would occur were frequently wrong and predictions for EMP current and voltage stress were subject to large errors (up to +/- 30 dB). System failures were predicted when none occurred, and conversely, no failures were predicted in cases where effects did occur. Pre-test predictions often missed the location—box, component—of system failure. The ELECTRA Technical Review Group concluded that methods used to predict EMP effects in a specific system that are based primarily on analysis or low-level testing are not reliable and recommended,

*Where reliable [electromagnetic effects] predictions for specific systems are required, protections should be based on high-level functional-response tests performed on the specific systems of interest.<sup>36</sup>*

---

<sup>34</sup> The ELECTRA Program's Technical Review Group's interim report of January 1995 includes a set of unclassified chapters on program methodology. See G.H. Baker, P. Castillo, C. McDonald, *et al.*, Electromagnetic Effects Comparison Test and Reliability Assessment (ELECTRA) Program: Executive Summary (U).

<sup>35</sup> ELECTRA Executive Summary (1995), p. iv.

<sup>36</sup> ELECTRA Executive Summary (1995), p. 49.

Further, where one or several complex system samples are subjected to high-level EMP injection testing, the test results can be prudently attributed to the larger population.<sup>37</sup> Thus, threat-level testing of even one sample is helpful to characterize the vulnerability and survivability of the larger set of systems. For large power transformers operating at 345 kV, 500 kV, and 765 kV voltages, for example, the DoD has the capability to transport EMP injection and diagnostic monitoring equipment to sites where these units are deployed. *In situ* testing to failure of exemplars of the major types of large power transformers under load would confirm whether specific types of large power transformers require EMP-protective equipment and enable new type transformer designs that resist EMP effects.

***Recommendation 5:*** *The Commission recommends that the Department of Defense and the Department of Energy provide expedited threat-level, full-system testing of large power transformers in wide use within the bulk electric system and share key findings with the electric utility industry.*

## INTELLIGENCE COMMUNITY ASSESSMENT OF THE EMP THREAT

Finally, the Commission found that the classified report by the Joint Atomic Energy Intelligence Committee (JAEIC) on EMP issued in 2014 is factually erroneous and analytically unsound.<sup>38</sup> We recommend that the DNI circulate to all recipients of the 2014 JAEIC report the EMP Commission critique and direct a new assessment be prepared, reviewed by experts in the subject areas being addressed, and circulated to all the recipients of the 2014 assessment.

***Recommendation 6:*** *The Commission recommends the Director of National Intelligence circulate to all recipients of the 2014 JAEIC report the EMP Commission critique and direct a new assessment be prepared that supersedes the 2014 JAEIC EMP report.*

---

<sup>37</sup> ELECTRA Executive Summary (1995), p. ii

<sup>38</sup> Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *Assessment of the 2014 JAEIC Report on High-altitude EMP Threats*, Report of the EMP Commission, July 2017.

## CONCLUSIONS

---

The critical national infrastructure in the United States faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, as well as from natural EMP from a solar superstorm. During the Cold War, major efforts were undertaken by the Department of Defense to assure that the U.S. national command authority and U.S. strategic forces could survive and operate after an EMP attack. However, no major efforts were then thought necessary to protect critical national infrastructures, relying on nuclear deterrence to protect them. With the development of small nuclear arsenals and long-range missiles by new, radical U.S. adversaries, the threat of a nuclear EMP attack against the U.S. becomes one of the few ways that such a country could inflict devastating damage to the United States. It is critical, therefore, that the U.S. national leadership address the EMP threat as a critical and existential issue, and give a high priority to assuring the leadership is engaged and the necessary steps are taken to protect the country from EMP.

Protecting and defending the national electric grid and other critical infrastructures from cyber and EMP could be accomplished at reasonable cost and minimal disruption to the present systems that comprise U.S. critical infrastructure. The following six recommendations are offered to accomplish this goal.

***Recommendation 1:*** *The Commission recommends the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat.*

***Recommendation 2:*** *The Commission strongly recommends that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection.*

***Recommendation 3:*** *The Commission encourages the President to work with Congressional leaders to establish a joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership to achieve, on an accelerated basis, the protection of critical national infrastructures.*

***Recommendation 4:*** *The Commission recommends that government agencies and industries adopt new standards to protect critical national infrastructures from damaging E3 EMP heave fields, with more realistic standards of 85 V/km.*

***Recommendation 5:*** *The Commission recommends that the Department of Defense and the Department of Energy provide expedited threat-level, full-system testing of large power transformers in wide use within the bulk electric system and share key findings with the electric utility industry.*

***Recommendation 6:*** *The Commission recommends the Director of National Intelligence circulate to all recipients of the 2014 JAEIC report the EMP Commission critique and direct a new assessment be prepared that supersedes the 2014 JAEIC EMP report.*



## APPENDIX A Legislation Re-establishing the Commission

---

**SEC. 1089. REESTABLISHMENT OF COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE ATTACK.**

(a) **REESTABLISHMENT.**—The commission established pursuant to title XIV of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (as enacted into law by Public Law 106-398; 114 Stat. 1654A-345), and reestablished pursuant to section 1052 of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109-163; 50 U.S.C. 2301 note), known as the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, is hereby reestablished.

(b) **MEMBERSHIP.**—Service on the Commission is voluntary, and Commissioners may elect to terminate their service on the Commission. If a Commissioner is unwilling or unable to serve on the Commission, the Secretary of Defense, in consultation with the chairmen and ranking members of the Committees on Armed Services of the House of Representatives and the Senate, shall appoint a new member to fill that vacancy.

(c) **COMMISSION CHARTER DEFINED.**—In this section, the term “Commission charter” means title XIV of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (as enacted into law by Public Law 106-398; 114 Stat. 1654A-345 et seq.), as amended by section 1052 of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109-163; 50 U.S.C. 2301 note) and section 1073 of the John Warner National Defense Act for Fiscal Year 2007 (Public Law 109-364; 120 Stat. 2403).

(d) **EXPANDED PURPOSE.**—Section 1401(b) of the Commission charter (114 Stat. 1654A-345) is amended by inserting before the period at the end the following: “, from non-nuclear EMP weapons, from natural EMP generated by geomagnetic storms, and from proposed uses in the military doctrines of potential adversaries of using EMP weapons in combination with other attack vectors.”.

(e) **DUTIES OF COMMISSION.**—Section 1402 of the Commission charter (114 Stat. 1654A-346) is amended to read as follows:

**“SEC. 1402. DUTIES OF COMMISSION.**

“The Commission shall assess the following:

“(1) The vulnerability of electric-dependent military systems in the United States to a manmade or natural EMP event, giving special attention to the progress made by the Department of Defense, other Government departments and agencies of the United States, and entities of the private sector in taking steps to protect such systems from such an event.

“(2) The evolving current and future threat from state and non-state actors of a manmade EMP attack employing nuclear or non-nuclear weapons.

“(3) New technologies, operational procedures, and contingency planning that can protect electronics and military systems from the effects of a manmade or natural EMP event.

“(4) Among the States, if State grids are protected against manmade or natural EMP, which States should receive highest priority for protecting critical defense assets.

“(5) The degree to which vulnerabilities of critical infrastructure systems create cascading vulnerabilities for military systems.”.

(f) **REPORT.**—Section 1403 of the Commission charter (114 Stat. 1654A-345) is amended by striking “September 30, 2007” and inserting “June 30, 2017”.

(g) **TERMINATION.**—Section 1049 of the Commission charter (114 Stat. 1654A-348) is amended by inserting before the period at the end the following: “, as amended by the National Defense Authorization Act for Fiscal Year 2016”.



## APPENDIX B High Altitude Nuclear Explosion-Generated Electromagnetic Effects

---

In the case of high altitude nuclear bursts, three main phenomena come into play, each with distinct associated system effects:

1. The first, a “prompt” EMP field, also referred to as E1, is created by gamma ray interaction with stratospheric air molecules. It peaks at tens of kilovolts per meter in a few nanoseconds, and lasts for a few hundred nanoseconds. E1’s broad-band power spectrum (frequency content in the 10s to 100s of megahertz) enables it to couple to electrical and electronic systems in general, regardless of the length of their penetrating cables and antenna lines. Induced currents range into the 1000s of amperes. Exposed systems may be upset or permanently damaged.
2. The second component of the EMP field, referred to as E2, is produced by delayed gamma rays and neutron-induced currents, lasts from microseconds to milliseconds, and has a magnitude in the hundreds of volts per meter. Its spectral characteristics are similar to those of naturally occurring lightning.
3. The third component, late-time EMP, also referred to as magnetohydrodynamic (MHD) EMP or E3, is caused by the distortion of the earth’s magnetic field lines due to the expanding nuclear fireball and rising of heated and ionized layers of the ionosphere. The change of the magnetic field at the earth’s surface induces currents of 100s-1000s of amperes in long conducting lines (a few kilometers or greater) that damage components of the electric power grid itself as well as connected systems. Long-line communication systems are also affected, including copper as well as fiber-optic lines with repeaters. Transoceanic cables are a prime example of the latter.

Solar storm geomagnetic disturbance (GMD) effects are the result of large excursions in the flux levels of charged particles from the Sun and their interactions with the Earth’s magnetic field and upper atmosphere. Perturbation of the Earth’s magnetic field, similar to MHD EMP, can generate overvoltages in long-line systems over large regions of the earth’s surface affecting electric power and communication transmission networks.

For each effect, directly-affected systems may be upset or permanently damaged. For unmanned systems and industrial control systems, upset effects can cascade to cause permanent damage to other connected systems. Wide-area electromagnetic system effects are challenging due to their near-simultaneous initial effects and cascading effects on a wide array of infrastructures. Infrastructure systems comprised of long-line conductor networks are the most vulnerable to both effects. Susceptible networks include the electric power grid, land-line communications, and interstate pipelines. Effects on these networks will cascade to most other

infrastructures. Smaller, self-contained, self-powered infrastructure systems (e.g. hand-held radios and vehicles) are also directly vulnerable, but only to EMP (not GMD) and to a lesser degree than long-line networks.

## BIOGRAPHIES

---

### COMMISSIONERS

**Dr. William R. Graham** is Chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. He was Chairman of the Board and Chief Executive Officer of National Security Research Inc. (NSR), a Washington-based company that conducts technical, operational, and policy research and analysis related to US national security. Previously he served as a member of several high-level study groups, including the Department of Defense Transformation Study Group, the Defense Science Board, the Commission to Assess United States National Security Space Management and Organization (the Rumsfeld Commission on Space), the Commission to Assess the Ballistic Missile Threat to the United States (also led by Hon. Donald Rumsfeld), and the National Academies' Board on Army Science and Technology. From 1986–89 Dr. Graham was the Director of the White House Office of Science and Technology Policy while he served concurrently as Science Advisor to President Reagan, Chairman of the Federal Joint Telecommunications Resources Board, and member of the Arms Control Experts Group. Before going to the White House, he served as the Deputy Administrator of NASA. For 11 years, he served as a member of the Board of Directors of the Watkins-Johnson Company.

**Dr. John S. Foster, Jr.** began his career at the Radio Research Laboratory of Harvard University in 1942 and then volunteered to be an advisor to the 15th Army Air Force on radar countermeasures in Italy. In 1952, Dr. Foster joined the Lawrence Livermore National Laboratory, designed nuclear weapons, became Director of that Laboratory, then in 1965 served as Director of Defense Research and Engineering for the Department of Defense until 1973. He joined TRW to work on energy programs and then served on the Board, retiring in 1988. He currently serves as a consultant to LLNL and an Advisor to STRATCOM SAG Panel. He has served on the Air Force Scientific Advisory Board, Army Scientific Advisory Panel, Ballistic Missile Defense Advisory Committee, and Advanced Research Projects Agency. From 1973 – 1990 he was a member of the President's Foreign Intelligence Advisory Panel. He served as Chairman of the Defense Science Board from 1990 to 1993. He served on the Congressional Commission on the Strategic Posture of the United States and on the Advisory Committee to the Director of DARPA.

**Mr. Earl Gjelde, P.E.**, is the Managing Director and Chief Executive Officer of Summit Group International, Ltd.; Summit Energy Group, Ltd.; Summit Energy International 2000, LLC; and Summit Power NW, LLC, primary participants in the development of over 5,000 megawatts of natural gas fired electric and wind generating plants within the United States. He has also held a number of government posts, serving as President George Herbert Walker Bush's Under (now called Deputy) Secretary and Chief Operating Officer of the US Department of the Interior (1989) and as President Ronald Reagan's Under Secretary and Chief Operating Officer of the US Department of the Interior (1985–1988). While in the Reagan administration he served

concurrently as Special Envoy to China (1987), Deputy Chief of Mission for the US-Japan Science and Technology Treaty (1987–1988), and Counselor for Policy to the Director of the National Critical Materials Council (1986–1988); the Counselor to the Secretary and Chief Operating Officer of the US Department of Energy (1982-1985); and Deputy Administrator, Chief Operating Officer, and Power Manager of the Bonneville Power Administration (1980-1982). Prior to 1980, he was a principal officer of the Bonneville Power Administration.

**Dr. Robert J. Hermann** is a senior partner of Global Technology Partners, LLC, a Boston-based investment firm that focuses on technology, defense aerospace, and related businesses worldwide. In 1998, Dr. Hermann retired from United Technologies Corporation, where he was Senior Vice President, Science and Technology. Prior to joining UTC in 1982, Dr. Hermann served 20 years with the National Security Agency with assignments in research and development, operations, and NATO. In 1977, he was appointed Principal Deputy Assistant Secretary of Defense for Communications, Command, Control, and Intelligence. In 1979, he was named Assistant Secretary of the Air Force for Research, Development, and Logistics and concurrently was Director of the National Reconnaissance Office.

**Mr. Henry (Hank) M. Kluepfel** served as Vice President for Corporate Development at SAIC, where he was the company's leading cyberspace security advisor to the President's National Security Telecommunications Advisory Committee (NSTAC) and the Network Reliability and Interoperability Council (NRIC). Mr. Kluepfel is widely recognized for his 30-plus years of experience in security technology research, design, tools, forensics, risk reduction, education, and awareness, and he is the author of industry's de facto standard security base guideline for the Signaling System Number 7(SS7) networks connecting and controlling the world's public telecommunications networks. In past affiliations with Telcordia Technologies (formerly Bellcore), AT&T, BellSouth and Bell Labs, he led industry efforts to protect, detect, contain, and mitigate electronic and physical intrusions and led the industry's understanding of the need to balance technical, legal, and policy-based countermeasures to the then emerging hacker threat. He has been recognized as a Certified Protection Professional by the American Society of Industrial Security and is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

**Gen Richard L. Lawson, USAF (Ret.),** served as Chairman of Energy, Environment and Security Group, Ltd., and as President and CEO of the National Mining Association. He also served as Vice Chairman of the Atlantic Council of the U.S.; Chairman of the Energy Policy Committee of the US Energy Association; Chairman of the United States delegation to the World Mining Congress; and Chairman of the International Committee for Coal Research. Active duty positions included serving as Military Assistant to the President; Commander, 8th Air Force; Chief of Staff, Supreme Headquarters Allied Powers Europe; Director for Plans and Policy, Joint Chiefs of Staff; Deputy Director of Operations, Headquarters US Air Force; and Deputy Commander in Chief, US European Command.

**Dr. Gordon K. Soper** served as the Group Vice President of Defense Group Inc., responsible for broad direction of corporate goals relating to company support of government customers in

areas of countering the proliferation of weapons of mass destruction, chemical/biological defense and domestic preparedness, treaty verification research, nuclear arms control and development of new business areas and growth of technical staff. He has also provided senior-level technical support on a range of task areas to the Defense Threat Reduction Agency (DTRA), the Chemical and Biological National Security Program of National Nuclear Security Administration, and the Counterproliferation and Chem/Bio Defense Office of the Office of the Secretary of Defense. Previously, Dr. Soper was Principal Deputy to the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Programs (ATSD (NCB); Director, Office of Strategic and Theater Nuclear Forces Command, Control and Communications (C3) of the Office of the Assistant Secretary of Defense (C3I); and Associate Director for Engineering and Technology/Chief Scientist at the Defense Communications Agency.

**Dr. Lowell L. Wood, Jr.** is retired from a career-long position on the technical staff of Lawrence Livermore National Laboratory, operated by the University of California for the U.S. Department of Energy, and an extended term as a Research Fellow of the Hoover Institution at Stanford University. Since his retirement a decade ago, Dr. Wood has continued part-time technical consulting in the commercial sector and serving as an External Advisor of the Bill & Melinda Gates Foundation, the world's largest private charity, focusing his efforts on global health and development. Dr. Wood holds the distinction of being the most inventive American in history, holding more U.S. patents on new inventions than any other person, including Thomas Edison, the previous record-holder.

**Dr. Joan Woodard** was Executive Vice President and Deputy Director of Sandia National Laboratories, responsible for all of Sandia's programs, operations, staff, and facilities. She was also responsible for the laboratory's strategic planning. Previously, Dr. Woodard was Vice President of the Energy, Information and Infrastructure Technology Division, where her responsibilities included energy-related projects in fossil energy, solar, wind, geothermal, geosciences, fusion, nuclear power safety and severe accident analysis, and medical isotope processing; environment-related programs in remediation, nuclear waste management and repository certification, and waste minimization; information technology programs in information surety, command and control systems, and distributed information systems; and programs responsible for security of the transportation of nuclear weapons and special nuclear materials, and safety of commercial aviation. Over 80 percent of the programs included industrial or academic partners, and the nature of the work ranged from basic research to prototype systems evaluation.

## SENIOR ADVISORS

**Dr. George H. Baker** is a Professor Emeritus at James Madison University, where he directed the JMU Institute for Infrastructure and Information Assurance. Previously, Dr. Baker led the Defense Nuclear Agency's Electromagnetic Pulse (EMP) program, directed the Defense Threat Reduction Agency's assessment arm, and served as a member of the Congressional EMP

Commission Staff. Dr. Baker holds an M.S. in Physics from University of Virginia, and a Ph.D. in Engineering Physics from the U.S. Air Force Institute of Technology. Currently, Dr. Baker is CEO of BAYCOR, LLC, and is Director of the Foundation for Resilient Societies.

**Mr. William R. Harris** is an international lawyer specializing in arms control, nuclear non-proliferation, energy policy, and continuity of government. He worked on Hot Line upgrades, creation of linked Nuclear Risk Reduction Centers, and was a co-drafter of arms limitation treaties in 1986-87, 1991, and 1993. Mr. Harris worked for the RAND Corporation and in a variety of assignments for the U.S. Government. Mr. Harris holds a B.A. from Harvard College and a J.D. from Harvard Law School. Mr. Harris serves as Secretary and attorney for the Foundation for Resilient Societies.

**Dr. Peter Vincent Pry** is a recognized expert on protection strategies for electromagnetic pulse (EMP) and related threats. In addition to his service for the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, he has served on the Congressional Strategic Posture Commission, as Executive Director of the U.S. Nuclear Strategy Forum and the Task Force on National and Homeland Security (both Congressional Advisory Boards); as Professional Staff on the House Armed Services Committee of the U.S. Congress, with portfolios in nuclear strategy, WMD, Russia, China, NATO, the Middle East, intelligence, and terrorism; as an Intelligence Officer with the Central Intelligence Agency; and as a Verification Analyst at the U.S. Arms Control and Disarmament Agency. Dr. Pry has written numerous books and articles on national security issues.

**Dr. William A. Radasky** is President and Managing Engineer at the Metatech Corporation. Metatech develops technically sound and innovative solutions to problems in all areas of electromagnetic environmental effects, including: electromagnetic interference and compatibility, geomagnetic storm assessments and protection, nuclear electromagnetic pulse prediction, assessments, protection and standardization, and intentional electromagnetic interference assessments, protection and standardization. Dr. Radasky has published over 400 technical papers, reports and articles dealing with electromagnetic interference (EMI) and protection. In 2004 he received the Lord Kelvin Award from the International Electrotechnical Commission for exceptional contributions to international standardization.

**Dr. David Stoudt** is a Senior Executive Advisor at Booz Allen where he provides leadership and guidance on the science and business of advancing directed energy capabilities for American warfighters. He previously spent 32 years serving in the Department of Navy, with deep experience in directed energy and electric weapon systems, including high-energy lasers, the electromagnetic rail gun, and high-power microwave weapon systems. Among other honors, David has received multiple Meritorious Civilian Service Awards, the Navy Distinguished and Superior Civilian Service Awards, and the Naval Sea Systems Command Scientist of the Year Award.

**Ambassador R. James Woolsey Jr., J.D.**, is a national security and energy specialist and former Director of Central Intelligence who headed the Central Intelligence Agency from



February 5, 1993, until January 10, 1995. A lawyer by training and trade, he held a variety of government positions in the 1970s and 1980s, including as Under Secretary of the Navy from 1977 to 1979, and was involved in treaty negotiations with the Soviet Union for five years in the 1980s, including as Chief Negotiator of the Conventional Forces in Europe Treaty.

## COMMISSION REPORTS

---

### REPORTS OF THE COMMISSION

Executive Report, 2004

Critical National Infrastructures Report, 2008

Assessing the Threat from EMP Attack: Executive Report, 2017

Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures, 2017

Assessment of the 2014 JAEIC Report on High-altitude Electromagnetic Pulse (HEMP) Threats,  
**SECRET//RD-CNWDI//NOFORN**, 2017

### STAFF PAPERS TO THE COMMISSION

G. Baker. Risk-Based National Infrastructure Protection Priorities for EMP and Solar Storms, 2017

W.R. Graham. Chairman's Report, 2017.

J. G. Kappenman and W.A. Radasky. Examination of NERC GMD Standards and Validation of Ground Models and Geo-Electric Fields, 2017

T.S. Popik, G.H. Baker, and W.R. Harris. Electric Reliability Standards for Solar Geomagnetic Disturbances, 2017

P.V. Pry. Nuclear EMP Attack Scenarios and Combined-arms Cyber Warfare, 2017

P.V. Pry. Political-Military Motives for Electromagnetic Pulse Attack, 2017

P.V. Pry. Foreign Views of Electromagnetic Pulse Attack, 2017

P.V. Pry. Life without Electricity: Storm Induced Blackouts and Implications for Electromagnetic Pulse Attack, 2017

P.V. Pry. Nuclear Terrorism and Electromagnetic Pulse Attack, 2017

E. Savage and W. Radasky. Late-Time (E3) HEMP Heave Parameter Study, **SECRET//RD**, 2017

# **LIFE WITHOUT ELECTRICITY: STORM-INDUCED BLACKOUTS AND IMPLICATIONS FOR EMP ATTACK**

by

Dr. Peter Vincent Pry

July 2017

Report to the Commission to Assess the Threat to the United States  
from Electromagnetic Pulse (EMP) Attack

REPORT TO THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES  
FROM ELECTROMAGNETIC PULSE (EMP) ATTACK

---

**LIFE WITHOUT ELECTRICITY:  
STORM-INDUCED BLACKOUTS AND  
IMPLICATIONS FOR EMP ATTACK**

by

**Dr. Peter Vincent Pry**

**July 2017**

This paper was drafted on June 20, 2003 to inform the work of the EMP Commission during 2001-2008, but could not be published because the Commission was terminated before Staff Papers could be submitted for security classification review. It is offered now for completeness of the analytical record.

The cover photo depicts Fishbowl Starfish Prime at 0 to 15 seconds from Maui Station in July 1962, courtesy of Los Alamos National Laboratory.

This report was produced to support the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. The Commission was established by Congress in the FY2001 National Defense Authorization Act, Title XIV, and was continued per the FY2016 National Defense Authorization Act, Section 1089.

The Commission completed its information-gathering in June 2017. The report was cleared for open publication by the DoD Office of Prepublication and Security Review on October 19, 2017.

This report is unclassified and cleared for public release.

**Table of Contents**

Summary .....2

Hurricane Lili (October 2002).....5

Hurricane Floyd (September 1999) .....7

Ice Storm Washington, D.C. (14 January 1999) .....8

The Great Ice Storm (January 1998).....9

Western Heat Wave (10 August 1996) .....12

Hurricane Andrew (August 1992) .....15



## Summary

Storm-induced blackouts of the electric power grid are suggestive of the possible consequences of an electromagnetic pulse (EMP) attack, such as could be made by rogue states or terrorists detonating a nuclear weapon at high-altitude over the United States. Electric power grid failure caused by storms cascade through other critical infrastructures—such as communications, transportation, emergency medical services, food and water supply systems. Storm-induced blackouts provide an objective basis for extrapolating judgments about the threat posed by EMP to the civilian infrastructures that sustain economic, political, and social life.

The vulnerability of critical infrastructures to various forms of attack has been a growing concern in recent years, drawing presidential attention in the Marsh Commission, and receiving additional impetus after the terrorist attacks of September 11<sup>th</sup> that moved President Bush to establish the Department of Homeland Security. However, the science of analyzing critical infrastructures, their interdependencies, and their possible vulnerabilities is relatively new. Much effort and significant resources have been invested in an inductive approach to understanding the potential for cascading failures through the critical infrastructures that may result from failure of the power grid. The prevailing approach relies heavily on complex mathematical calculations, theoretical models, and computer simulations.

Analysis of storm-induced blackouts and their consequences offers an empirical approach that complements the predominant inductive approach to understanding infrastructure interdependence and vulnerability. Moreover, beyond the interdependence and potential vulnerability of critical infrastructures, analysis of storm-induced blackouts provides some empirical basis for estimating the effects of infrastructure failure on social order.

Storm-induced blackouts are an imperfect analogy to EMP attack from nuclear weapons of high-yield or special design. Taken at face value, storm-induced blackouts and their consequences grossly understate the threat posed by EMP attack. Storms are much more limited in geographic scope compared to EMP attack. So power grid recovery from storms, compared to recovery from EMP attack, is likely to be faster because of the “edge effect”—the capability of neighboring localities and states to provide recovery assistance. Because EMP attack is likely to damage or disrupt electronics over a much wider geographic area than storm-induced blackouts, rescuers from neighboring states and localities would face a much bigger job, and recovery probably would take a much longer time.

Nor do storm-induced blackouts replicate the damage from an EMP attack that may occur in small-scale electronic systems such as computers, aircraft, and automobiles. Compared to storms, nuclear weapons of high-yield or special design are likely to inflict, not only more widespread damage geographically, but deeper damage, affecting a much broader spectrum of electronic equipment.

Storms are merely suggestive of, and provide some basis for extrapolating, the greater destructive effects on infrastructures and social order by an EMP attack from a nuclear weapon

of high-yield or special design. Storm-induced blackouts and their consequent physical damage to other infrastructures may well be equivalent to an EMP attack from a nuclear weapon of low-yield and primitive design, such as terrorists might be able to build. In this latter case, storm-induced blackouts and the cascading physical effects on other infrastructures may be taken as representative of the lowest, and most benign, level of the EMP threat spectrum.

However, although some storms may be equivalent to a primitive EMP attack in their physical damage to the power grid and other infrastructures, storms probably understate even a primitive EMP attack in its psychological dimensions. Unlike EMP attack, hurricanes and other storms are familiar to the public and understood to be acts of nature, not the destructive agents of a foreign enemy. Public perceptions of and reactions to mass destruction differ markedly when the agent of destruction is a familiar natural event or accident, versus destruction by unfamiliar means inflicted deliberately by malignant actors. For example, the American people endure tornadoes and hurricanes without mass panic, and accept with equanimity 50,000 deaths yearly from automobile accidents. But the same number of deaths inflicted over a decade by a foreign enemy was enough to cause a political and cultural revolution in the United States, and broke the will of the people and political elites who accepted defeat in the Vietnam War. More recently, the 3,000 deaths and other destruction inflicted by the terrorist attacks of September 11 have moved the United States, with wide popular support, to prosecute successful wars in Afghanistan and Iraq as part of a broader ongoing war against terrorism. The United States government and people support this effort because, although U.S. society can survive the worst hurricane, the September 11 events forged a new consensus that U.S. society, and civilization itself, may not be able to survive future terrorist attacks.

Psychologically benign though storms may be, compared to terrorist attacks that inflict lesser or greater physical destruction, even storms challenge social order. This survey has found that some storm-induced blackouts have caused crime waves and disintegrated organized communities into disorganized refugees, for example.

Significantly, some observers of storm-induced blackouts—even when blackouts lasted only a day or two, as is commonly the case—were struck by the potential fragility of modern society and its near total dependence upon electricity. For example, a January 1999 ice storm that blacked-out electricity in the Washington, D.C. area moved the **Washington Post** to note that “daily life was crippled, if not halted—dramatically illustrating the fragile dependence of modern times on the flip of a switch.”<sup>1</sup> The *Post* continued:

*Automated teller machines were out, as were gasoline pumps at many service stations. WETA-TV (Channel 26) went black for more than 10 hours until employees found a diesel generator to put that station back on the air. The Montgomery County jail conducted bond hearings by flashlight. Families seeking refuge at Tysons Corner Center were booted out at 6 p.m. because of*

---

<sup>1</sup> Susan Levine and Tom Jackman, “Region Iced Over and Blacked Out,” **Washington Post** (16 January 1999), p. A1.

*water problems at the mall....Up and down Metro's Red Line, riders confronted stalled elevators, inoperable Farecard machines and even closed stations. Negotiating roads...was often no easier. Of more than 700 traffic signals in Montgomery, 430 were dead. Across the area, but especially in Montgomery, hotels filled to capacity with customers fleeing cold, dark homes. The 365-room Doubletree Hotel on Rockville Pike was sold out by 8 a.m.....Other residents, with pioneering spirit, decided to ride out the outage. More than two dozen people were waiting when the Home Depot in Germantown opened at 6 a.m.. By 10 a.m., the store had sold every generator, log of firewood, candle, kerosene heater and any other supply that could warm hands and feet.<sup>2</sup>*

Another dramatic example of the dependency of social order upon electricity occurred in October 2002, during the aftermath of Hurricane Lili that blacked-out much of coastal Louisiana. In some areas, the absence of street lights caused "looting and vandalism bad enough to require enforcement of a dusk-to-dawn curfew."<sup>3</sup> Local police had to be reinforced by police from neighboring localities in order to cope with the crime wave. "The looting," remarked Abbeville Mayor Mark Piazza, "Is not expected to go away until the lights come on."<sup>4</sup>

Some experts claim that an EMP attack that collapses the power grid would, in effect, return society to a pre-industrial condition. A February 1987 snowstorm that blacked-out the Washington, D.C. area suggested exactly this to many of its victims. According to press reports, people were reduced to using open fires for heat, cooking and, in some areas, melting snow for water. Homes with fireplaces became havens for multiple families seeking refuge from houses heated by electric, gas, or oil that no longer worked. As she "stoked a fire and began sterilizing water for her baby's formula," one woman told reporters, "It's like the Colonial days."<sup>5</sup>

Storm-induced blackouts are localized and last usually no more than a day or two. Yet they can momentarily return part of our society to technological primitivism and begin cracks in the social order. Compared to storms, the consequences of an EMP attack would be far graver. Compared to the worst storms, an EMP attack would probably destroy infrastructures more completely within a region and over a much larger region—perhaps over the entire continental United States. An EMP attack, compared to the worst storms, would probably inflict more lasting damage—requiring perhaps weeks or months to repair.

Therefore, we can reasonably infer from the data on storm-induced blackouts and the known greater severity of high-altitude nuclear EMP that the consequences of an EMP attack on the United States' infrastructures and society would be an unprecedented and first order catastrophe.

---

<sup>2</sup> Ibid.

<sup>3</sup> Leslie Williams, "One Town's Battle," **Times-Picayune** (9 October 2002), p. 1.

<sup>4</sup> Ibid.

<sup>5</sup> John Lancaster and Chris Spolar, "Washington's Wet Blanket," **Washington Post** (24 February 1987), p. 1.

Some of the salient infrastructure and social consequences of storm-induced blackouts are listed below. Not all of the failures and effects described occurred during all storms. This survey was careful to select only failures and effects traceable to power grid failure. Failures and effects resulting from phenomenon other than electric power grid blackout (downed trees, flooding and etc.) are not reported here. Storm- and weather-related blackouts examined in this survey include Hurricane Lili (2002), Hurricane Floyd (1999), the Washington Ice Storm of 1999, the Great Ice Storm of 1998, the Western Heat Wave of 1996, and Hurricane Andrew (1992):

- **Social Order:** Looting requires dusk to dawn curfew. People become refugees as they flee powerless homes. Work force becomes differently employed at scavenging for basics, including water, food, and shelter.
- **Communications:** No TV, radio, or phone service.
- **Transportation:** Gas pumps inoperable. Failure of signal lights and street lights impedes traffic, stops traffic after dark. No mass transit metro service. Airlines stopped.
- **Water and Food:** No running water. Stoves and refrigerators inoperable. People melt snow, boil water, and cook over open fires. Local food supplies exhausted. Most stores close due to blackout.
- **Energy:** Oil and natural gas flows stop.
- **Emergency Medical:** Hospitals operate in dark. Patients on dialysis and other life support threatened. Medications administered and babies born by flashlight.
- **Death and Injury:** Casualties from exposure, carbon dioxide poisoning and house fires increase.
- **Edge Effect:** Recovery depends heavily on neighboring regions unaffected by blackout. For example, Louisiana rescued from Hurricane Lili blackout by 14,000 workers from 24 states.

### Hurricane Lili (October 2002)

Hurricane Lili struck the coast of Louisiana on October 3, 2002, coming ashore at Vermillion Bay, the eye of the storm centered on Abbeville about 90 minutes after landfall.<sup>6</sup> Lili knocked down 35 transmission lines and destroyed 53 electric power substations.<sup>7</sup> More than 500,000 people were without electric power at the height of the blackout, immediately after the storm.<sup>8</sup> Three days later, on October 6, over 100,000 homes and businesses were still without power in coastal Louisiana, according to the state Office of Emergency Preparedness.<sup>9</sup> Six days after Lili, on October 9, in Abbeville and surrounding Vermillion Parish, an estimated 80 percent of the 20,000 homes and 50 percent of businesses were still without electricity.<sup>10</sup>

---

<sup>6</sup> Williams, op. cit., p. 1.

<sup>7</sup> Angela Simoneaux, "Flooded, Battered La. Gets Busy Cleaning Up," **Morning Advocate** (5 October 2002), p. 1A.

<sup>8</sup> Angela Simoneaux, "Acadiana's Recovery," **The Advocate** (8 October 2002), p. 5B.

<sup>9</sup> Kevin McGill, "Rise Seen In Carbon Monoxide Poisoning Cases," **The Advocate** (7 October 2002), p. 2B.

<sup>10</sup> Williams, op. cit., p. 1.

As a consequence of the blackout, water and food were unavailable through the normal means to thousands. With no electricity, water pumping stations no longer worked. In south Louisiana, 30 supermarkets would not open because the blackout prevented their cash registers from operating. Those grocery stores that did open were stripped of food within hours. In Abbeville, the parking lots of shopping centers became watering and feeding stations run by churches and the state Office of Emergency Preparedness. Associated Grocers, that supplies food to supermarkets in Louisiana, Texas, and Mississippi, sent food and refrigerated trucks to the stricken area. The food emergency was reflected in a skyrocketing demand for dry ice to preserve food stuffs during the hot weather and to preserve refrigerated foods. Local supplies of dry ice were exhausted—one store selling 20,000 pounds of dry ice to hundreds of customers in two hours—and had to be supplemented with supplies from the Red Cross.<sup>11</sup>

The electrical outage deprived thousands of phone service for days after the Hurricane.<sup>12</sup> Television service was also blacked out.<sup>13</sup>

The blackout interfered with transportation by rendering signal lights inoperable.<sup>14</sup> Street lights were also inoperable, making driving at night difficult even for long-time local residents, who could not see landmarks and became disoriented in the dark.<sup>15</sup>

Power grid collapse caused failure in other energy infrastructures. Without electricity, natural gas service could not be restored for several days after Lili.<sup>16</sup>

Many hospitals were plunged into darkness during the blackout because they had no emergency generators or emergency power systems failed to work. There was no hot water for bathing patients or sterilization. “We have to give them medicines in the dark,” said one nurse, “We use a flashlight to make sure we don’t give them the wrong one.”<sup>17</sup>

The blackout caused indirectly some injuries and at least one death. Home generators used by people who lost power after Hurricane Lili led to more than 60 cases of carbon monoxide poisoning, including one fatality, according to Louisiana health officials.<sup>18</sup>

Some officials and citizens considered the blackout the worst part of Hurricane Lili. According to Mayor Chuck Butterfield, “We’ve taken electricity for granted and living without it for three or four days is devastating.”<sup>19</sup> Law enforcement officers blamed a surge of looting and vandalism on the blackout. The crime wave became bad enough to require the imposition of a dusk-to-dawn curfew and police reinforcements from neighboring areas unaffected by the storm.

---

<sup>11</sup> Simoneaux, “Acadiana’s Recovery,” p. 5B. Williams, op. cit., p. 1. Simoneaux, “Flooded, Battered La. Gets Busy Cleaning Up,” p. 1A. Suzan Manuel, “Lili Leaves Residents Powerless,” *Daily Town Talk* (5 October 2002), p. 1A. Suzan Manuel, “Thousands Still Without Electricity Across Central La.,” *Daily Town Talk* (6 October 2002), p. 8A.

<sup>12</sup> McGill, op. cit., p. 2B.

<sup>13</sup> Simoneaux, “Acadiana’s Recovery,” p. 5B.

<sup>14</sup> Manuel, “Lili Leaves Residents Powerless,” p. 1A.

<sup>15</sup> Williams, op. cit., p. 1.

<sup>16</sup> McGill, op. cit., p. 2b.

<sup>17</sup> Manuel, “Lili Leaves Residents Powerless,” p. 1A.

<sup>18</sup> McGill, op. cit., p. 2B.

<sup>19</sup> Manuel, op. cit. p. 8A.

“The looting,” according to the Abbeville Sherriff’s Office, “Is not expected to go away until the lights come back on.”<sup>20</sup>

Recovery from the blackout, described by a CLECO electric utility spokesman as “the biggest customer outage event in our history,” depended heavily on outside assistance.<sup>21</sup> Some 14,000 electric utility workers from 24 states and the District of Colombia joined CLECO’s 3,000 workers to make recovery possible in about one week.<sup>22</sup>

### **Hurricane Floyd (September 1999)**

Expected to be a “killer storm” of rare power and destruction, when Hurricane Floyd made landfall near Cape Fear, North Carolina on September 16, 1999, it had subsided into a tropical storm that inundated much of the east coast with heavy rainfall and flooding. But there was little of the destruction anticipated by federal and state authorities that had prompted them to evacuate over 3 million people from the hurricane’s path.<sup>23</sup>

Floyd did blackout electrical grids in many areas. However, the consequences of those blackouts for other infrastructures and for society are difficult to evaluate since blackouts tended to occur in areas where the population had already evacuated. Blackouts did interrupt phone service in North Carolina.<sup>24</sup> In Salisbury, North Carolina, more than 200 of 1,200 supermarkets were put out of operation by protracted blackouts, causing substantial food spoilage despite emergency efforts undertaken before the storm to preserve perishable goods in freezers.<sup>25</sup> Most cable TV customers lost service in Baltimore due to a blackout.

Floyd blackouts are notable for causing water treatment and sewage plants to fail in some Virginia localities and, most notably, in Baltimore. Blackout induced failure of Baltimore’s Hampden sewage facility for several days raised concerns about a threat to public health. With its three pumps inoperable, Hampden spilled 24 million gallons of waste into Baltimore’s Jones Falls waterway and the Inner Harbor.<sup>26</sup>

Perhaps Floyd’s blackouts are most significant for complicating the largest evacuation and return of civilians in United States history. Electrical outages apparently prevented many from finding shelter—some traveled over 500 miles seeking accommodations, and found none. Blackout induced failure of traffic signals contributed to some of the largest traffic jams in the

---

<sup>20</sup> Williams, op. cit., p. 1.

<sup>21</sup> Simoneaux, “Flooded, Battered La. Gets Busy Cleaning Up,” p. 1A.

<sup>22</sup> Keith Darce, “Lights Blink Out All Over Louisiana,” **Times-Picayune** (4 October 2002), p. 1. “Lili Left Half A Million Without Power,” **Associated Press** (4 October 2002).

<sup>23</sup> Brad Liston, Melissa August, Delphine Matthieussent, and Timothy Roche, “A Very Close Call,” **Time** (27 September 1999), p. 34.

<sup>24</sup> Amanda Milligan Hoffman and Sally Roberts, **Business Insurance** (Crain Communications: 1999).

<sup>25</sup> Ibid.

<sup>26</sup> Governors James Hunt and James Gilmore interviewed, “Hurricane Floyd Leaves Lingering Questions About Public Policy,” **CNN Crossfire** (16 September 1999). Del Quentin Wilber, “Jones Falls Sewage Spill Lasts 2 Days,” **Baltimore Sun** (19 September 1999), p. 1A.



nation's history as evacuees tried to return home. For example, one traffic jam on Interstate 10 from the Carolinas to Florida stretched 200 miles.<sup>27</sup>

### **Ice Storm Washington, D.C. (14 January 1999)**

On January 14, 1999, an ice storm downed 250 high-voltage power lines in Washington D.C. and the neighboring suburbs in Maryland and Northern Virginia, causing what the Potomac Electric Power Company (PEPCO) described as "the worst power outage in the utility's 102-year history."<sup>28</sup> The blackout left 435,000 homes and businesses without power. Recovery took six days.<sup>29</sup>

Warm food, potentially a survival issue in the freezing winter conditions, was not available in most people's homes because electric ovens and microwaves no longer worked. Most gas-powered ovens also would not work because those built since the mid-1980s have electronic ignition and cannot be lit with a match.<sup>30</sup> Some resorted to cooking on camp stoves. Preserving refrigerated foods was also a concern that PEPCO tried to help address by giving away 120,000 pounds of dry ice, all it had.<sup>31</sup> Dry ice became a precious commodity.<sup>32</sup>

The blackout crippled ground and rail transportation. Gasoline pumps were rendered inoperable. Non-functioning traffic lights snarled traffic:

*Up and down Metro's Red Line, riders confronted stalled elevators, inoperable fare card machines and even closed stations. Negotiating roads...was often no easier. Of more than 700 traffic signals in Montgomery, 430 were dead....Arlington County motorcycle officers proved especially resourceful, borrowing portable generators from the public library system to help run traffic lights at four major intersections.*<sup>33</sup>

A local television station, WETA-TV, went off the air for more than 10 hours because of the blackout.<sup>34</sup>

At least one hospital was blacked out. Babies were born by flashlight.<sup>35</sup> Emergency medical services suffered to such an extent that patients requiring life support were put at risk, PEPCO admitted:

<sup>27</sup> Liston and et. al., op. cit., p. 34. Aaron Steckelberg, "Scenes From The Coast," **Atlanta Constitution** (16 September 1999), p. 10A.

<sup>28</sup> Scott Wilson, "From Ice Storm To Firestorm," **Washington Post** (31 January 1999), p. A1. Manuel Perez-Rivas, "Six-Day Power Outage Is Over," **Washington Post** (21 January 1999), p. B1.

<sup>29</sup> Ibid.

<sup>30</sup> Phillip P. Pan and Spencer S. Hsu, "Without Power, Thousands Wait In Hotels, Malls And Cold Homes," **Washington Post** (17 January 1999), p. A1.

<sup>31</sup> Perez-Rivas, op. cit., p. B1.

<sup>32</sup> Wilson, op. cit. (31 January 1999), p. A1.

<sup>33</sup> Susan Levine and Tom Jackman, "Region Iced Over and Blacked Out," **Washington Post** (16 January 1999), p. A1.

<sup>34</sup> Ibid.

<sup>35</sup> Wilson, op. cit. (31 January 1999), p. A1.

*The extent of damage caused by last week's ice storm prevented PEPCO and other area utilities from giving priority to customers with serious medical conditions, including those on life-support systems or dialysis machines, company executives said yesterday.*<sup>36</sup>

Ice storm induced blackout in freezing conditions posed a threat to life. Hypothermia surged among the elderly, trapped in their unheated homes. People tried to stay warm by burning charcoal indoors, causing an increase in carbon monoxide poisoning and house fires:

*At least a dozen houses...in Montgomery were damaged by fires caused by residents' efforts to stay warm or cook...after burning charcoal indoors. More than a hundred people spent Friday night in emergency shelters...Hospitals reported an influx of elderly in their emergency rooms.*<sup>37</sup>

In Maryland, the blackout moved Governor Parris Glendening to declare a state of emergency in six counties. The Governor activated the National Guard to assist firehouses.<sup>38</sup>

The power outage created a refugee population “of entire neighborhoods...searching for warmth and diversion at hotels, theaters, malls and even office towers.”<sup>39</sup> Thousands were “fleeing cold, dark homes,” according to press reports:

*Across the area, but especially in Montgomery, hotels filled to capacity with customers fleeing cold, dark homes. The 365-room Doubletree Hotel on Rockville Pike was sold out by 8 a.m.. Residence Inn by Marriott, on Wisconsin Avenue in Bethesda, with 187 rooms, was sold out by noon.*<sup>40</sup>

The blackout moved the **Washington Post** to observe that “daily life was crippled, if not halted—dramatically illustrating the fragile dependence of modern times on the flip of a switch.”<sup>41</sup>

### **The Great Ice Storm (January 1998)**

Starting on January 4<sup>th</sup> and for six days, until January 10, 1998, freezing rain fell across a 600-mile weather front that included parts of Ontario and Quebec in Canada, and Maine and upstate New York in the United States. Electric outages in the affected areas of Canada deprived 4.7 million people, or 16 percent of the Canadian population, of power, according to Emergency Preparedness Canada. In the United States, 546,000 people were without power (deprived of heat, light, and in many instances water) in the cold of mid-winter.<sup>42</sup>

---

<sup>36</sup> Scott Wilson, “Utilities Say Blackout Overwhelmed Medical Priorities,” **Washington Post** (22 January 1999), p. B3.

<sup>37</sup> Pan and Hsu, op. cit., p. A1.

<sup>38</sup> Ibid.

<sup>39</sup> Ibid.

<sup>40</sup> Ibid. Levine and Jackman, op. cit., p. A1.

<sup>41</sup> Levine and Jackman, op. cit., p. 1.

<sup>42</sup> Eugene L. Lecomte, Alan W. Pang, and James W. Russell, **Ice Storm '98** (Institute for Business and Home Safety: December 1998), pp. 1-2.

Some of the 5.2 million people affected by the Great Ice Storm of 1998 went without power for five weeks. It was the greatest natural disaster in Canadian history, and generated more insurance claims than Hurricane Andrew, the costliest natural disaster in U.S. history.<sup>43</sup>

One historian of the Great Ice Storm notes that “the storm’s biggest impact was, in a sense, not weather-related: It was the loss of electricity”:

*Ice accumulations caused the collapse of more than a thousand...transmission towers...More than 7,500 transformers stopped working....Some parts of Monteregie, a region of 1.3 million people southeast of Montreal, went without power for so long that the area became known as “the Dark Triangle.”*<sup>44</sup>

The blackout caused an immediate and life-threatening emergency in Montreal’s water supply that depended upon electricity for filtration and pumping. At 12:20 P.M. on January 9<sup>th</sup>, the two water filtration plants that served 1.5 million people in the Montreal region went down, leaving the area with only enough water to last 4 to 8 hours. Government officials kept the water crisis secret, fearing public knowledge would exacerbate the crisis by water hoarding. However:

*Even as officials deliberated, water pipes in some households were already dry. As reports and rumors of a water shortage spread, consumption jumped by 10 percent anyway, and bottled water disappeared from stores.*<sup>45</sup>

The **Toronto Star**, in an article entitled “Millions Shiver In Dark: How A Major City is Being Crippled by Deadly Ice Storm,” reported that parts of Montreal had run out of water, “and those who still had it were warned not to drink tap water without boiling it first.”<sup>46</sup> But most people had no way of boiling water.

Officials feared not only a shortage of drinking water, but an inadequate supply of water for fighting fires. So desperate was the situation that Alain Michaud, Fire Chief of Montreal, prepared to fight fires with a demolition crane instead of water, hoping that “if a building caught fire, it might burn to the ground, but the crane would demolish neighboring structures to prevent the fire’s spread.”<sup>47</sup> By 9:30 P.M. on January 9<sup>th</sup>, one of Montreal’s major reservoirs was nearly empty. Provincial officials considered evacuating the city. However, Hydro-Quebec, the government electric utility, managed to restore power to the filtration plants and restore water service.<sup>48</sup>

The blackout also threatened the food supply: “Food poisoning has become a real threat as embattled Montrealers, unable to get to stores, eat food that has been kept too long in

---

<sup>43</sup> Jacques Leslie, “Powerless,” **Wired** (April 1999), p.120.

<sup>44</sup> Ibid.

<sup>45</sup> Ibid, p. 176.

<sup>46</sup> Sandro Contenta, “Millions Shiver In Dark: How A Major City Is Being Crippled By Deadly Ice Storm,” **Toronto Star** (10 January 1998), p. A1.

<sup>47</sup> Leslie, op. cit., p. 176.

<sup>48</sup> Ibid.

refrigerators that don't work."<sup>49</sup> In upstate New York, the electric utility Niagara Mohawk announced that it was focusing restoration of electric power on more populated areas "so that supermarkets, gasoline stations and hotels could reopen, and people in the more rural areas could find food and shelter."<sup>50</sup> New York State Electric and Gas helped customers get to shelters and distributed 200,000 pounds of dry ice for storing food."<sup>51</sup> One typical resident of Canada's "Dark Triangle" complained, "I've lost all my food...I melt ice for water. It's no way for a family to live."<sup>52</sup>

Shelter, another basic necessity for survival, was also threatened by the mid-winter blackout: "People without power discovered just how many facets of their lives depended on electricity. Their stoves, appliances, and heating didn't work."<sup>53</sup> Many of Canada's newer, well-insulated homes relied on inexpensive electric heat.<sup>54</sup> Thousands of people fled their cold, dark homes to seek refuge in government and charitable shelters. The situation in Saint-Jean-sur-Richelieu, a working-class town of 36,000 was typical, where 3,600 people became shelter refugees, one-tenth of the population.<sup>55</sup> St. Hyacinthe in the "Dark Triangle" lost nearly half its residents, who mostly fled the city.<sup>56</sup> About 100,000 people took refuge in shelters.<sup>57</sup>

Communications, financial, and transportation infrastructures failed massively during the blackout. In upstate New York, only French Canadian radio stations were still on the air. In Ontario, 50,000 telephones went dead, frustrating the electric utility from restoring power service, since it relied on customer phone calls to locate power failures. Credit cards and ATM machines became useless, so all financial transactions had to be in cash.<sup>58</sup> The blackout shut down Montreal's four subway lines for the first time in the system's 30-year history.<sup>59</sup>

Underscoring that the blackout, not the ice storm, was the real crisis, the Canadian Premier Lucien Bouchard declared that "the most urgent need" was for generators, and appealed to anyone in Canada with a generator to help.<sup>60</sup> Bouchard also appealed to the U.S. Federal Emergency Management Agency, "asking for beds and generators to provide shelters with heat and light."<sup>61</sup>

Hospitals in Canada and the United States were nearly overwhelmed with blackout victims. In Maine, where six out of ten residents lost power, a single hospital, in Lewiston, reported

---

<sup>49</sup> Contenta, op. cit., p. A1.

<sup>50</sup> "Monster Ice Storm Slays Transmission Facilities In Quebec, Upstate New York," **Northeast Power Report** (McGraw-Hill: 16 January 1998), p. 1.

<sup>51</sup> "Canada And New England Still Reeling," **Electric Utility Week** (19 January 1998), p. 1.

<sup>52</sup> Jack Beaudoin, "Quebec In Crisis," **Portland Press Herald** (8 February 1998), p. 45.

<sup>53</sup> Leslie, op. cit., p. 176.

<sup>54</sup> Beaudoin, op. cit., p. 45.

<sup>55</sup> Leslie, op. cit., p. 178.

<sup>56</sup> Beaudoin, op. cit., p. 45.

<sup>57</sup> Leslie, op. cit., p. 122.

<sup>58</sup> Ibid, p. 176.

<sup>59</sup> Contenta, op. cit., p. A1.

<sup>60</sup> Mark Dunn, "Ice Storm Holds Eastern Ontario In Its Beautiful But Deadly Grip," **The Record** (9 January 1998), p. A1.

<sup>61</sup> Contenta, op. cit., p. A1.

treating for carbon monoxide poisoning 120 people “who ran generators, kerosene heaters and even charcoal grills in their homes to keep warm.”<sup>62</sup>

Hospital medical services underwent a crisis during the protracted blackout when their emergency generators failed. For example, at Montreal’s LeMoyne Hospital:

*The generators broke down on the sixth day, and the staff instantly switched to flashlights. For two hours until the generators were repaired, the hospital lost the use of its life-support and monitoring equipment: Nurses pumped air by hand into the lungs of patients on respirators and manually took each patient’s pulse and blood pressure every 15 minutes. Instead of one nurse for each six patients, a ratio of at least one-to-one was needed.*<sup>63</sup>

The blackout indirectly caused hundreds of deaths in Canada and the U.S., according to Great Ice Storm historian Jacques Leslie. Leslie criticizes the official death toll figures as too low:

*The official death toll was 45-28 fatalities in Canada, 17 in the U.S.—but those numbers understate the ice storm’s effects. Hundreds of ill and elderly people, weakened by extended stays in shelters where flu became epidemic, died weeks or months later, succumbing to ailments they might otherwise have overcome.*<sup>64</sup>

Over a year after the Great Ice Storm ended, according to Jaques Leslie, “The people who experienced it remain aware of one overriding lesson: Their dependence on electricity makes them more vulnerable than they’d ever imagined.”<sup>65</sup> Mark Abley, author of **The Ice Storm**, makes a similar observation:

*Huddling in school gyms, church halls, shopping malls, and other shelters, the evacuees didn’t pray for a return of fine weather. They prayed for a return of power. The ice storm demonstrated not that we are prisoners of brutal weather, but that we are all now hostages to electricity.*<sup>66</sup>

### **Western Heat Wave (10 August 1996)**

A heat wave, with near record high temperatures, blacked out large parts of nine western states on a torrid Saturday afternoon, August 10<sup>th</sup>, 1996. Near-record high temperatures covered most of the West at the time: for example, over 100 degrees in eastern Oregon and the San Joaquin Valley, 113 degrees in Red Bluff, and 104 degrees in Boise, Idaho.<sup>67</sup> Initial speculation that the blackout was sparked by a brushfire near Oregon was later discounted. According to

<sup>62</sup> Peter Pochna and Abby Zimet, “Facing Down An Ice Storm,” **Portland Press Herald** (18 January 1998), p. 1A.

<sup>63</sup> Leslie, op. cit., pp. 178, 180.

<sup>64</sup> Ibid, pp. 122-123.

<sup>65</sup> Ibid, p. 123.

<sup>66</sup> Ibid.

<sup>67</sup> Rich Connell, “Massive Power Outage Hits Seven Western States,” **Los Angeles Times** (11 August 1996), p. 1.

Dulcy Mahar, spokeswoman for the Bonneville Power Administration, the blackout was caused by the heat wave:

*Some of the lines sagged because of the heat. Some of those lines sagged down onto trees and then tripped off for safety reasons. The power that those lines were carrying was moved off to other lines and overloaded those, and then the safety devices tripped those lines off and you had the outages.*<sup>68</sup>

Although the blackout lasted less than 24 hours, it was “one of the largest power outages on record.”<sup>69</sup> The blackout affected “an estimated 4 million people in nine states, trapping people in elevators, snarling traffic and generally causing widespread chaos.”<sup>70</sup> The blackout caused problems that could have become a significant threat to life and society, had they been more protracted.

Water supplies were interrupted in some regions because electric pumps would not work. Arizona, New Mexico, Oregon, Nevada, Texas, and Idaho experienced blackout-induced disruption in water service during the heat wave. For example:

*In Fresno, where most of the city receives water from wells powered by electric pumps, the city manager declared a local emergency. Only two of the city’s 16 fire stations had water sources and most of the fire hydrants were out. The county and Air National Guard rushed in tankers to boost the Fire Department’s capacity.*<sup>71</sup>

Air and ground transportation systems experienced significant disruptions because of the blackout. For example, at San Francisco International Airport, although an emergency generator powered the control tower, other systems—security, computers, elevators, and luggage carousels—would not work. Jetways could not be positioned at airplane doors. An estimated 6,000 passengers were stranded.<sup>72</sup> Incoming flights had to be diverted to San Jose and Oakland. Airport Spokesman Bob Schneider announced, “We are pretty much out of business.”<sup>73</sup>

Signal lights failed, causing massive traffic jams in San Francisco and San Diego. “Traffic is a nightmare,” declared San Francisco Police Department spokesman Bruce Metdors, “They’re just backed up everywhere. It’s gridlock.”<sup>74</sup> San Francisco mass transit—electric trolleys and BART metro trains—were stalled by the blackout.<sup>75</sup> “We’re responding in what amounts to our earthquake mode,” said Orange County Fire Captain Dan Young, “We certainly had an increase

<sup>68</sup> Tim Golden, “Power Failure in 6 Weeks Creates Havoc for the West,” *New York Times* (12 August 1996), p. 13. See also Tina Griego, “Regulators Will Take Up Western Power Failures,” *Albuquerque Tribune* (12 August 1996), p. A1.

<sup>69</sup> Connell, op. cit., p. 1.

<sup>70</sup> Robert Dintleman, “Western Power Failures Traced To Soaring Temperatures,” *All Things Considered, National Public Radio* (11 August 1996), Transcript #2302-5.

<sup>71</sup> Connell, op. cit., p. 1.

<sup>72</sup> Ray Delgado, “Huge Blackout Hits West Coast,” *San Francisco Examiner* (11 August 1996), p. A1.

<sup>73</sup> Connell, op. cit., p. 1.

<sup>74</sup> Ibid.

<sup>75</sup> Delgado, op. cit., p. A1.



in traffic collisions, since you've got thousands of signals with no control on them.”<sup>76</sup> Gas pumps were out of order, stranding motorists who needed to refuel. “All the pumps run on electricity,” explained one station attendant, “When you think about it, everything runs on electricity.”<sup>77</sup>

“Even a few hours without electricity caused chaos,” according to press reports:

*Los Angeles police went on a citywide tactical alert as supervisors ordered some day shift officers to stay on duty into the night. Firefighters patrolled the city, responding to dozens of reports of stuck elevators. Department of Transportation crews checked on 4,000 intersections where the outage could have put traffic lights on the fritz. Blaring fire alarms and broken water lines added to the havoc.*<sup>78</sup>

Communications were disrupted by the blackout. “Radio stations reported power outages at locations throughout the midsection of California,” according to press reports, “In San Francisco, TV stations KPIX and KQED were off-line for some time due to the outage.”<sup>79</sup> Radio Station KNBR and the Canadian Broadcast Corporation went off the air.<sup>80</sup> Cable television networks crashed.<sup>81</sup>

Emergency medical services were disrupted by the blackout because “trauma rooms across the state [California] were cut off for hours from the radio that tells them an emergency is heading their way.”<sup>82</sup> Fire crews equipped with portable power generators were sent to doctors’ offices so the physicians could complete surgeries.<sup>83</sup> In Orange County, 200 fire units were dedicated to providing power to hospitals with emergency vehicles.<sup>84</sup>

The blackout disrupted control systems in some major industrial facilities. For example, the Chevron refinery in Richmond, California, “was unable to control flues due to the outage,” releasing “huge clouds of black smoke.”<sup>85</sup> The blackout caused power plants throughout the west—“including nuclear plants near Central California’s Morro Bay and west of Phoenix”—to shut down.<sup>86</sup> The Diablo Canyon nuclear power plant, near San Luis Obispo, shut down, and required several days for technicians to complete safety checks before it could be started again.<sup>87</sup>

---

<sup>76</sup> Kim Boatman and Lori Aratani, “Millions Lose Power,” **San Jose Mercury News** (11 August 1996), p. 1A.

<sup>77</sup> Marilyn Kalfus, Ana Menendez, and Julio Laboy, “Blackout Brings Much Of O.C. To A Halt,” **Orange County Register** (11 August 1996), p. A1.

<sup>78</sup> Connell, op. cit., p. 1.

<sup>79</sup> Delgado, op. cit., p. 1.

<sup>80</sup> Boatman and Aratani, op. cit., p. A1.

<sup>81</sup> Kalfus and et. al., op. cit., p. A1.

<sup>82</sup> Ibid.

<sup>83</sup> Douglas E. Beeman, “Hot West Goes Dim,” **The Press Enterprise** (11 August 1996), p. A1.

<sup>84</sup> Jim Hill, “West Coast Power Outage Easing In Some Locations,” **Show, CNN** (10 August 1996), Transcript #1600-4.

<sup>85</sup> Delgado, op. cit., p. 1.

<sup>86</sup> Beeman, op. cit., p. A1.

<sup>87</sup> Golden, op. cit., p. 13.

The Bonneville Power Administration told the press, “All of the utilities are relying on each other, and it has a cascading effect when one part experiences a major failure.”<sup>88</sup>

### **Hurricane Andrew (August 1992)**

Hurricane Andrew struck southern Florida on August 24, 1992 and reached the coast of Louisiana on August 26, two days later. Andrew has been described by some experts as the worst natural disaster in U.S. history.<sup>89</sup> Andrew laid waste to 165 square miles in South Florida, destroying some 100,000 homes in Florida and Louisiana, and leaving more than 3.3 million homes and businesses without electricity.<sup>90</sup>

Federal and state officials were at first unaware of the magnitude of the disaster and slow to react. Three days into the crisis, Kate Hale, the Director of Dade County’s Office of Emergency Management called a press conference to demand of state and federal authorities, “Where the hell is the cavalry on this one? We need food. We need water. We need people. For God’s sake, where are they?”<sup>91</sup>

By the end of the first week, President Bush had ordered 14,400 troops into the Florida disaster area “with mobile kitchens, tents, electrical generators, water and blankets....Even those lucky enough to have homes may not have electricity for more than a month.”<sup>92</sup>

Andrew’s aftermath posed an immediate threat to life in South Florida because of damage to the infrastructures for water and food. A widespread electrical blackout prevented pumps from working, so there was no running water.<sup>93</sup> Most grocery stores had been destroyed. Massive traffic jams, caused in part by non-functioning signal and street lights, prevented the surviving supermarkets from being re-supplied. To meet the crisis, the Army Corps of Engineers distributed more than 200,000 gallons of water and the Department of Agriculture gave out tons of surplus food.<sup>94</sup> Nonetheless, two weeks after the hurricane, food was still not reaching many victims. On September 7, fifteen days after Andrew struck, reporters witnessed the following scene:

*In the ruins, Charlie Myers, 65, stood holding a peach and a loaf of bread.  
“This is all I have left, he said. What plans did he have? “Survive buddy.”<sup>95</sup>*

Andrew’s blackout of the power grid made the crisis over water, food, and shelter worse by severing communications between relief workers and victims. Without power, there was an

---

<sup>88</sup> Delgado, op. cit., p. 1.

<sup>89</sup> “Mother Nature’s Angriest Child,” **Time** (7 September 1992), p. 15.

<sup>90</sup> Tom Mathews, Peter Katel, Todd Barrett, Douglas Waller, Clara Bingham, Melinda Liu, Steven Waldman, and Ginny Carrol, “What Went Wrong,” **Newsweek** (7 September 1992), p. 23.

<sup>91</sup> Ibid.

<sup>92</sup> “Mother Nature’s Angriest Child,” op. cit., p. 16.

<sup>93</sup> William Booth and Mary Jordan, “Hurricane Rips Miami Area, Aims at Gulf States,” **Washington Post** (25 August 1992), p. A7.

<sup>94</sup> Mathews and et. al., op. cit., p. 27.

<sup>95</sup> Ibid.

almost complete collapse of communications—no phones, radio or television.<sup>96</sup> “Without electricity to power radio and television sets, mass communication remains difficult or impossible,” according to authorities and press reports.<sup>97</sup> Consequently, people were unaware of relief efforts or of where to go for help. For example, although the U.S. Marines erected “tent cities” able to accommodate thousands of homeless hurricane victims, many did not know of this refuge: “Many people in the vast storm-stricken area, even those who live within easy walking distance of the sprawling encampment, said they were not aware of the tents’ existence.”<sup>98</sup> Unable to communicate where victims could get water, relief workers stacked “pyramids of bottled water...on street corners, free for the taking.”<sup>99</sup>

The blackout of power and communications, according to press reports, imbued “South Florida with an end-of-the world aura”:

*Hundreds of thousands of people found themselves in a Stone Age existence, left to pursue hunting and gathering, forced to forage for food and water. Because many people in the devastated areas had no radios or batteries, the location of food distribution sites has been a mystery....Each time word spread about establishment of a new relief outlet, people suddenly would swarm forward on foot, and National Guard troops often had to be summoned to keep order. The hurricane robbed steamy South Florida of the two amenities deemed essential to life here: air conditioning and ice cubes. “We can’t stand this heat any longer,” said Rita Larraz, whose house in South Dade County was spared but who, like 750,000 customers here, still had no electricity, and therefore no air conditioning in the 90-plus degree heat and humidity...”The heat is killing us.”<sup>100</sup>*

The blackout crippled the transportation infrastructure, further impeding relief efforts. “More than 5,000 traffic lights are on the blink...,” according to press reports. Consequently, “Traffic was snarled for miles. The simplest chore, indeed almost everything, seemed to take forever.”<sup>101</sup>

Andrew’s blackout of the power grid contributed significantly to societal anarchy in South Florida. With the blackout induced collapse of communications there was no way for survivors of Andrew to report crimes in progress. An orgy of looting provoked vigilantism. Unable to rely on the police, individuals armed themselves to protect their homes and remaining possessions.

<sup>96</sup> One report indicates the phone system continued to operate or experienced only partial failure. See John Mintz, “Phones Withstand Hurricane’s Fury,” **Washington Post** (26 August 1992), p. F1. For a different view see Booth and Jordan, op. cit. (25 August 1992), p. A7.

<sup>97</sup> Laurie Goodstein and William Booth, “Marines Ready Tent Cities in South Florida,” **Washington Post** (1 September 1992), p. A1.

<sup>98</sup> Ibid.

<sup>99</sup> Ibid.

<sup>100</sup> William Booth, “Hurricane’s Fury Left 165 Square Miles Pounded Into the Ground,” **Washington Post** (30 August 1992), p. A1.

<sup>101</sup> Goodstein and Booth, op. cit., p. A1.

“Andrew had made one zone of society come unglued,” according to **Newsweek**, “Disasters penetrate like lasers, revealing weaknesses beneath the smooth surfaces of a community.”<sup>102</sup> Lack of streetlights encouraged “thieves...to take advantage of a general feeling of lawlessness, particularly before federal troops began arriving”:

*At night, in darkened streets cordoned by National Guard troops enforcing a curfew, machine-gun fire has been heard. Spray-painted on the side of a house in Perrine was: “I’m armed and dangerous! Looters shot on sight!” “Everyone is armed, everyone is walking around with guns,” said Navy physician Sharon Wood, who worked at a mobile hospital in Homestead, where workers refused to dispense calming drugs such as valium for fear that word might get out and the hospital might be robbed. In Kendall, senior citizens sleep at night with revolvers by their sides....Miami and its surrounding municipalities, which have a long history of racial and ethnic tension, were considered a tinderbox.*<sup>103</sup>

Some 3,300 National Guard troops enforced a dusk-to-dawn curfew, when looting was worst, under cover of darkness. More than 200 people were arrested for looting or violating the curfew.<sup>104</sup> However, some efforts to restore law and order impeded relief efforts:

*Roadblocks set up to stop looters continued to hamper delivery of emergency food supplies. Truckers with emergency food aid were forced to wait for police escorts after reports that some drivers had been shot and beaten by thugs. State troopers thwarted the progress of some private help when they began stopping all trucks entering the state, demanding that the drivers show that they and their cargo had been officially requested and that they were from a recognizable organization.*<sup>105</sup>

Ultimately, some 16,000 federal troops from every branch of the armed forces turned the lights back on and restored order to South Florida.<sup>106</sup>

---

<sup>102</sup> Mathews and et. al., op. cit., p. 24.

<sup>103</sup> Booth, op. cit., p. A18.

<sup>104</sup> William Booth and Mary Jordan, “Painful Awakening in South Florida,” **Washington Post** (26 August 1992), p. A27.

<sup>105</sup> Mary Jordan, “President Orders Military to Aid Florida,” **Washington Post** (28 August 1992), p. A14.

<sup>106</sup> Rick Gore, “Andrew Aftermath,” **National Geographic** (April 1993), p. 20.

VOLUME II

# **Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures**

**JULY 2017**

**Report of the Commission to Assess the Threat to the United States  
from Electromagnetic Pulse (EMP) Attack**





# Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures

**July 2017**

REPORT OF THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES  
FROM ELECTROMAGNETIC PULSE (EMP) ATTACK

---

The cover photo depicts Fishbowl Starfish Prime at 0 to 15 seconds from Maui Station in July 1962, courtesy of Los Alamos National Laboratory.

This report is a product of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. The Commission was established by Congress in the FY2001 National Defense Authorization Act, Title XIV, and was continued per the FY2016 National Defense Authorization Act, Section 1089.

The Commission completed its information-gathering in June 2017. The report was cleared for open publication by the DoD Office of Prepublication and Security Review on April 9, 2018.

This report is unclassified and cleared for public release.

TABLE OF CONTENTS

---

EXECUTIVE SUMMARY ..... 1

1 INTRODUCTION ..... 2

2 GROUND CONDUCTIVITY PROFILES ..... 7

3 SOVIET E3 HEMP MEASUREMENTS ..... 9

    Test Parameters..... 9

    Scaling of the Results..... 19

    Latitude Scaling..... 19

    Pattern Scaling..... 20

4 CONCLUSIONS..... 24

## LIST OF FIGURES

---

Figure 1	Parts of HEMP. E3 HEMP heave is roughly described by the second peak in the MHD signal. [SOURCE: Meta R-321]	3
Figure 2	Diagram of the E3 HEMP heave effect. [SOURCE: Meta R-321]	4
Figure 3	Sample normalized yield variation for maximum E field for heave for burst heights between 130 and 170 km and for a fixed Earth conductivity profile. [SOURCE: Meta R-321]	5
Figure 4	Sample normalized HOB variation for maximum peak E field for heave for an intermediate yield weapon and for a fixed Earth conductivity profile. [SOURCE: Meta R-321]	6
Figure 5	Ground conductivity depth profile for three ground profiles.	7
Figure 6	Ground profile B-to-E conversion in the frequency domain for three cases.	8
Figure 7	Simulation of the Soviet tests showing B field peaks and field directions, 150 km test (R2).	10
Figure 8	Simulation of the Soviet tests showing B field peaks and field directions, 300 km test (R1).	11
Figure 9	Measured B fields at N1, 150 km test.	12
Figure 10	Measured B fields at N2, 150 km test.	12
Figure 11	Measured B fields at N3, 150 km test.	13
Figure 12	Measured B fields at N1, 300 km test.	13
Figure 13	Measured B fields at N2, 300 km test.	14
Figure 14	Measured B fields at N3, 300 km test.	14
Figure 15	E field amplitudes for four ground profiles, at N1, 150 km test.	16
Figure 16	E field amplitudes for four ground profiles, at N2, 150 km test.	16
Figure 17	E field amplitudes for four ground profiles, at N3, 150 km test.	17
Figure 18	E field amplitudes for four ground profiles, at N1, 300 km test.	17
Figure 19	E field amplitudes for four ground profiles, at N2, 300 km test.	18
Figure 20	E field amplitudes for four ground profiles, at N3, 300 km test.	18
Figure 21	Geomagnetic latitude variation, for a 150 km burst, over the U.S. The black line is at $48.92^\circ$ , which is the computed geomagnetic latitude for the 150 km Soviet test.	20
Figure 22	Normalized simulated B field peaks versus ground range for the 150 km test. The black dot shows the simulated results for the N3 point.	21
Figure 23	Normalized simulated B field peaks versus ground range for the 300 km test. The black dot shows the simulated results for the N3 point.	22
Figure 24	E field waveform shape, using the measured N1 waveform from the 150 km burst height	24
Figure 25	Normalized E peak contour pattern from the 150 km burst case	25

LIST OF TABLES

---

Table 1    Geometry for the Soviet High-Altitude Tests. ....9

Table 2    Peaks of the Soviet measurement waveforms. (The E field is for the 10<sup>-3</sup> S/m  
ground.) ..... 15

Table 3    Geomagnetic latitude scaling of the Soviet measurements. ....21

Table 4    Pattern (observer position) scaling of the Soviet measurements.....22

Table 5    Scaling of the Soviet Measurements.....24

## ACRONYMS AND ABBREVIATIONS

---

B	magnetic field
CONUS	continental United States
DoD	Department of Defense
E	electric field
EMP	electromagnetic pulse
EPRI	Electric Power Research Institute
FERC	Federal Energy Regulatory Commission
GMD	geomagnetic disturbance
HEMP	high-altitude electromagnetic pulse
HOB	height of burst
km	kilometer
m	meter
MHD	magnetohydrodynamic
min	minute
NERC	North American Electric Reliability Corporation
nT	nanotesla
S/m	siemens/m
UV	ultraviolet
V	Volt



## PREFACE

---

This EMP Commission Report, utilizing unclassified data from Soviet-era nuclear tests, establishes that recent estimates by the Electric Power Research Institute (EPRI) and others that the low-frequency component of nuclear high-altitude EMP (E3 HEMP) are too low by at least a factor of 3. Moreover, this assessment disproves another claim--often made by the U.S. Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), EPRI and others—that the FERC-NERC Standard for solar storm protection against geo-magnetic disturbances (8 volts/kilometer, V/km) will also protect against nuclear E3 HEMP. A realistic unclassified peak level for E3 HEMP would be 85 V/km for CONUS as described in this report. New studies by EPRI and others are unnecessary since the Department of Defense has invested decades producing accurate assessments of the EMP threat environment and of technologies and techniques for cost-effective protection against EMP. The best solution is for DoD to share this information with industry to support near-term protection of electric grids and other national critical infrastructures that are vital both for DoD to perform its missions and for the survival of the American people.

## EXECUTIVE SUMMARY

---

As described in this report, there is a need to have bounding information for the late-time (E3) high-altitude electromagnetic pulse (HEMP) threat waveform and a ground pattern to study the impact of these types of electromagnetic fields on long lines associated with the critical infrastructures. It is important that this waveform be readily available and useful for those working in the commercial sectors.

While the military has developed worst-case HEMP waveforms (E1, E2, and E3) for its purposes, these are not available for commercial use. Therefore, in this report openly available E3 HEMP measurements are evaluated from two high-altitude nuclear tests performed by the Soviet Union in 1962. Using these data waveforms and an understanding of the scaling relationships for the E3 HEMP heave phenomenon, bounding waveforms for commercial applications were developed.

Since the measured quantities during these tests were the magnetic fields, it is possible to compute the electric fields assuming ground conductivity profiles that produce significant levels. There are other profiles that would compute even higher electric fields, but some of these profiles do not cover a very large area of the Earth.

After computing the electric fields using the Soviet measurements, the results were scaled to account for the fact that their measurement locations were not at the optimum points on the ground to capture the maximum peak fields. Through this process, it was determined that the scaled maximum peak E3 HEMP heave field would have been 66 volts per kilometer (V/km) for the magnetic latitude of the Soviet tests.

As the E3 HEMP heave field also increases for burst points closer to the geomagnetic equator, the measured results were also evaluated for this parameter. This scaling increases the maximum peak electric field up to 85 V/km for locations in the southern part of the continental U.S., and 102 V/km for locations nearer to the geomagnetic equator, as in Hawaii. The levels in Alaska would be lower at an estimated peak value of 38 V/km (see Table 5 for information dealing with this scaling process).

It is noted that this report does not claim that the values provided here are absolute worst-case field levels, but rather these peak levels are estimated based directly on measurements made during Soviet high-altitude nuclear testing.

## 1 INTRODUCTION

---

Over many years beginning in the 1980s, the U.S. has worked to establish the peak field levels, ground patterns of the heave portion of the late-time E3 HEMP fields as shown in Figure 1, and from these to build useful models.<sup>1,2</sup> In the summer of 1994, Soviet scientists attending the European Electromagnetics (EUROEM) Symposium in Bordeaux, France, presented several papers indicating their understanding of the different types of EMP including the high-altitude electromagnetic pulse (HEMP). One of the most interesting developments of that conference was that these presentations summarized the Soviet high-altitude electromagnetic test results and indicated that the most important aspects of the effects they observed were caused by the “long tail” of the HEMP.<sup>3</sup> In later publications, they indicated that the long tail referred to the late-time HEMP, or the E3 HEMP magnetohydrodynamic (MHD)-EMP heave signal, and later provided detailed technical information indicating that the failure of one long-haul communications line was due to this portion of the HEMP.<sup>4</sup> Three other references dealing with E3 HEMP (MHD-EMP) were published by Soviet scientists in this time frame presumably due to their interest in understanding the failures of commercial long line systems during their 1962 high-altitude nuclear testing program over Kazakhstan.<sup>5,6,7</sup>

Later in the early 2000s, Soviet scientists provided the EMP Commission with a memo that illustrated their magnetic field measurements of the E3 HEMP heave signals at three locations during two of their high-altitude nuclear tests over Kazakhstan in 1962.<sup>8</sup> Because the Soviets tested over land instead of over ocean, as did the U.S., several long line systems were affected by the E3 HEMP fields. In addition, measurements of the magnetic fields were made at several locations on the ground at various ranges from the surface zero (the point directly underneath the high-altitude burst).

- 
- <sup>1</sup> J. Gilbert, J. Kappenman, W. Radasky and E. Savage, “The Late-Time (E3) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid,” Meta R-321, January 2010.
  - <sup>2</sup> J.L. Gilbert, W.A. Radasky, K.S. Smith, K. Mallen, M.L. Sloan, J.R. Thompson, C.S. Kueny and E. Savage, “HEMPTAPS/HEMP-PC Audit Report,” Meta R-131, December 1999; DTRA-TR-00-1, April 2002.
  - <sup>3</sup> V.M. Loborev, “Up to Date State of the NEMP Problems and Topical Research Directions,” Proceedings of the European Electromagnetics International Symposium -- EUROEM 94, June 1994, pp. 15-21.
  - <sup>4</sup> V.N. Greetsai, A.H. Kozlovsky, V.M. Kuvshinnikov, V.M. Loborev, Y.V. Parfenov, O.A. Tarasov and L.N. Zdoukhov, “Response of Long Lines to Nuclear High-Altitude Nuclear Pulse (HEMP),” IEEE Transactions on EMC, Vol. 40, Issue 4, 1998, pp. 348-354.
  - <sup>5</sup> V.N. Greetsai, V.M. Kondratiev, and E.L. Stupitsky, “Numerical Modelling of the Processes of High-Altitude Nuclear Explosion MDH-EMP Formation and Propagation,” Roma International Symposium on EMC, September 1996, pp. 769-771.
  - <sup>6</sup> “The Physics of Nuclear Explosions,” Ministry of Defense of the Russian Federation, Central Institute of Physics and Technology, Volumes 1 and 2, ISBN 5-02-015124-6, 1997. MHD-EMP topics are found in Sections 13.5 and 13.6.3.
  - <sup>7</sup> V.M. Kondratiev and V.V. Sokovikh, “Redetermination of MHD-EMP Amplitude Characteristics and Spatial Distribution on the Ground Surface,” Roma International Symposium on EMC, September 1998, pp. 129-132.
  - <sup>8</sup> “Characteristics of magnetic signals detected on the ground during the Soviet nuclear high-altitude explosions,” memorandum provided by Soviet scientists, February 2003.

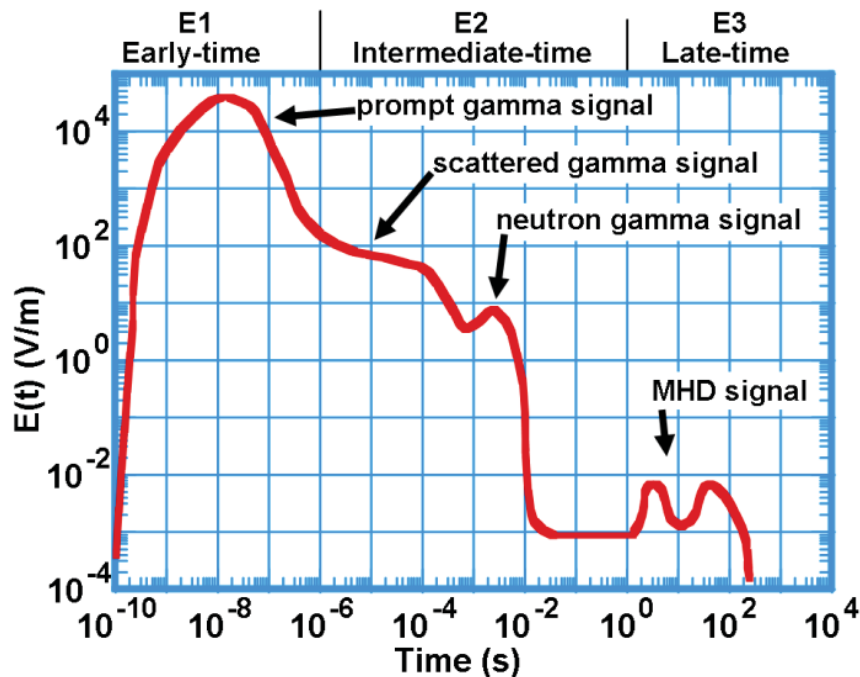


Figure 1 Parts of HEMP. E3 HEMP heave is roughly described by the second peak in the MHD signal. [SOURCE: Meta R-321]

In this report, the Soviet magnetic field data is reviewed, and through the use of several different ground conductivity profiles for locations in the U.S., the electric fields at the Earth's surface that could be induced are calculated. The magnetic fields are created by the nuclear detonation and the electric fields are induced in the earth and vary due to the particular deep conductivity profiles in the Earth. In addition, the magnetic fields (and electric fields) were also scaled to account for the fact that the Soviet measurements were not at the optimum ground locations to obtain the maximum peak fields on the ground. Finally, the increases in peak fields that would occur due to the well understood scaling of E3 HEMP with magnetic latitude were estimated, as the latitude of the Soviet tests were not at the bounding locations on the Earth.

The objective of this report is to determine from open source information how high the electric fields could be at latitudes of interest for the United States. In addition, a ground pattern and typical normalized electric field waveform is estimated that could be used for studies to determine the levels of quasi-DC currents that could be induced in long-line systems such as the bulk power system.

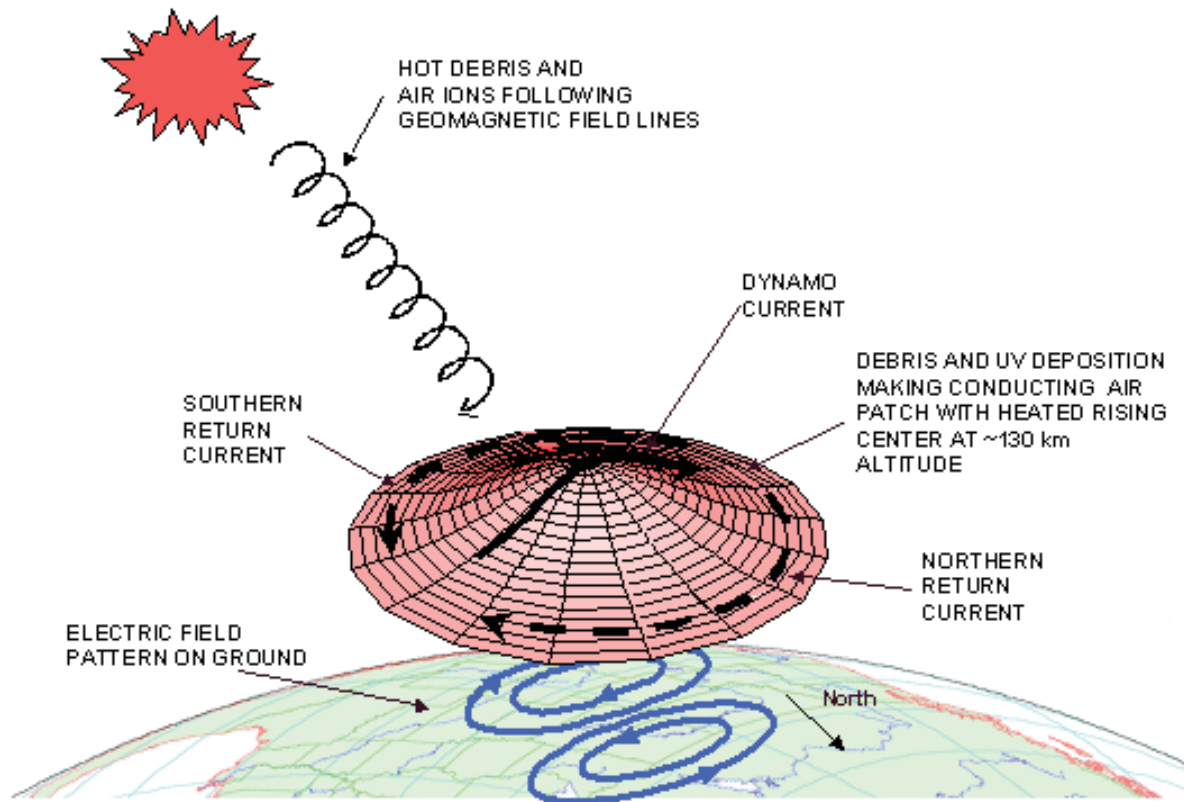
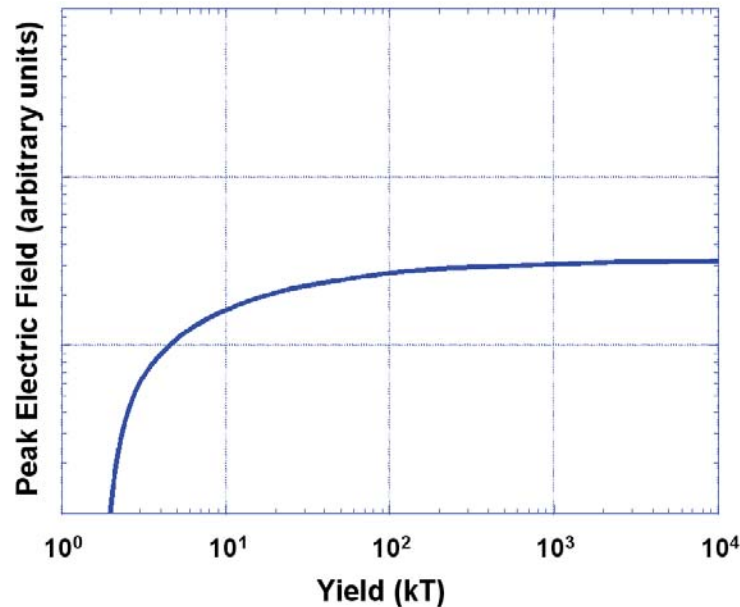


Figure 2 Diagram of the E3 HEMP heave effect. [SOURCE: Meta R-321]

This report does not claim that the values suggested here are absolute worst-case field levels, but rather these peak levels are estimated based directly on measurements made during high-altitude nuclear testing.

Figure 2 represents the E3 HEMP heave generation process. Hot ionized debris streaming downward away from the burst is directed preferentially along the geomagnetic field lines. As the debris and ultraviolet (UV) radiation from the burst reach altitudes where the atmosphere becomes dense enough, they heat up a “patch” of the atmosphere, and also add ionization to the background ionization already present in the ionosphere. The heat causes expansion, and the ionized region rises due to buoyancy. The Lorentz force on the ions and free electrons moving upward in the Earth’s geomagnetic field leads to east-west dynamo currents, with return currents completing the current flow on the north and south side. These currents induce image currents, with the associated electric fields, in the conductivity of the Earth below. Associated with this are magnetic (B) fields. The levels of the generated E fields are dependent on the actual ground conductivity to great depths of the Earth below the heaving patch, while the associated B field perturbations are approximately independent of the ground profile. For



*Figure 3 Sample normalized yield variation for maximum E field for heave for burst heights between 130 and 170 km and for a fixed Earth conductivity profile. [SOURCE: Meta R-321].*

this reason, the measured B fields on the Earth's surface can be considered to be the principal E3 HEMP heave environment.

It is noted that there is a second mechanism that creates E3 HEMP fields on the ground called "Blast Wave", but while it also can produce significant B fields, the maximum fields are found thousands of kilometers away from ground zero. For this reason, the Blast Wave phenomenon is not considered in this report.

The E3 HEMP heave B field perturbation on the ground depends on many parameters, such as:

1. Burst parameters: The characteristics of the burst are important. Of primary importance is the burst yield—bigger bombs would tend to have more debris coming down and generating the E3 HEMP heave signal. Figure 3 shows a sample of E3 HEMP heave variation with yield. This yield dependence can vary with the burst height. In addition, the area of coverage for the peak field tends to be larger for larger yields.
2. Burst location: The burst location has two important effects. First, the height of burst (HOB) is important for E3 HEMP heave, as it is for other HEMP phenomena. The precise interaction with the atmosphere depends on how high the burst is above the atmosphere. Also, the higher the burst, the farther north (for northern hemisphere bursts) the heated patch is found, as it needs to travel a further distance on the tilted



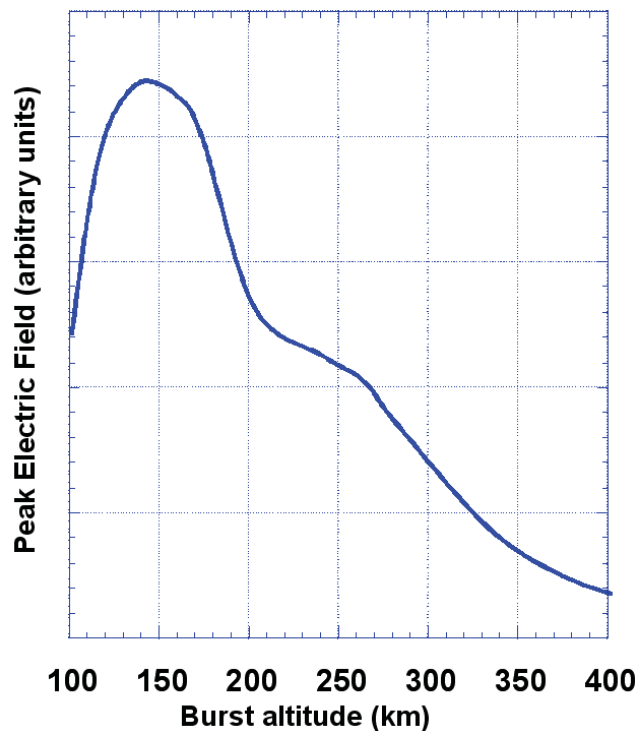


Figure 4 Sample normalized HOB variation for maximum peak E field for heave for an intermediate yield weapon and for a fixed Earth conductivity profile. [SOURCE: Meta R-321].

geomagnetic field lines. Figure 4 shows a sample of HOB variation for a fixed yield and ground conductivity profile. The other important location effect is the local geomagnetic field, which is represented by the value of geomagnetic latitude. One effect is that E3 HEMP heave gets weaker as the burst gets closer toward the (geomagnetic) poles, because the geomagnetic field becomes less horizontal, and there is less east-west deflection of the rising hot ions. (The geomagnetic latitude also affects the tilt of the path that the debris follows downward from the burst.)

3. Observer location: As seen in Figure 2, there is a 2-loop pattern of ground fields. The magnitude of the ground fields decreases with distance from the point directly below the patch. Examples of ground patterns are provided later in this report.
4. Burst time of day: Here the important factor is the “atmosphere”, basically the state of the ionosphere, which can vary significantly. Depending on the burst time, the day of the year, and the location, the burst may be in “night” or “day”. Sun exposure enhances the ionization of the ionosphere. For the E3 HEMP Blast Wave (the early-time portion of the E3 HEMP, which is not the subject of this report) the enhancement due to the “daytime” conditions depresses the E3 HEMP Blast Wave field, while for E3 HEMP heave there is an enhancement of the fields.

## 2 GROUND CONDUCTIVITY PROFILES

The E3 HEMP signal of concern in this report is the induced horizontal electric (E) field, as this field can effectively couple to long power and communications lines and induce quasi-dc currents in these systems. This coupling process has been discussed in several references including one that deals with geomagnetic disturbances (GMDs); GMD electric fields are similar in their time and frequency content to the electric fields produced by the E3 HEMP heave.<sup>9</sup> These E fields are produced by the presence of the conductivity depth profile in the Earth itself. For E3 HEMP heave it is the conductivity down to great depths (400-700 km) below the Earth's surface that determines the electric field. The E3 HEMP generation process begins with magnetic field (B) perturbations (relative to the geomagnetic field created by the Earth's core), and at the Earth's surface these B fields are little affected by the ground conductivity profile. Thus both calculations and measurements for actual nuclear tests typically begin with the B fields, and then E fields can be calculated for any assumed ground conductivity profile. While the induced peak E field is strongly related to the time derivative (dB/dt) of the horizontal B field, these calculations use the full Maxwell's Equations to determine the electric fields. The resulting E field is also horizontally oriented. The calculation of E from B must be done in terms of vector components—a B field in one horizontal direction creates an E field that is perpendicular to it under an assumed one-dimensional approximation for the local Earth conductivity profile.

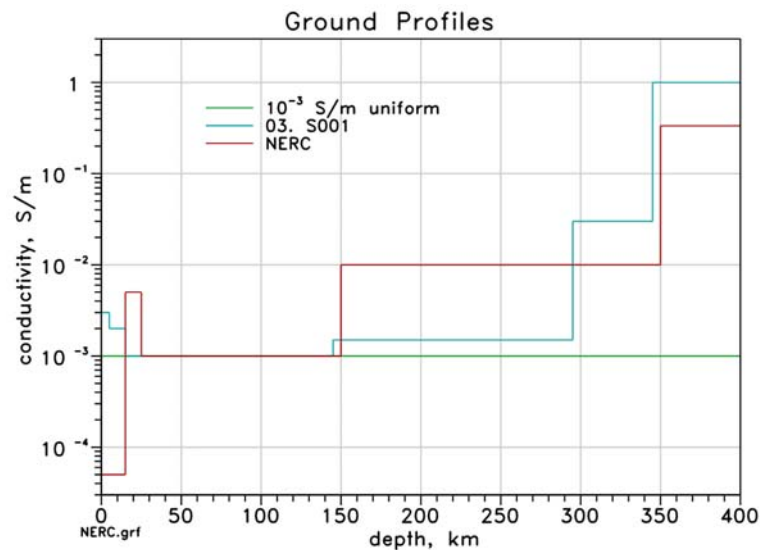


Figure 5 Ground conductivity depth profile for three ground profiles.

Figure 5 shows three ground profiles of ground conductivity with depth used in this report. The NERC profile (red line) has four layers of various conductivity levels, ending at a high

<sup>9</sup> W.A. Radasky, "Overview of the Impact of Intense Geomagnetic Storms on the U.S. High Voltage Power Grid," IEEE Electromagnetic Compatibility Symposium, Long Beach, California, 15-19 August 2011, pp. 300-305.

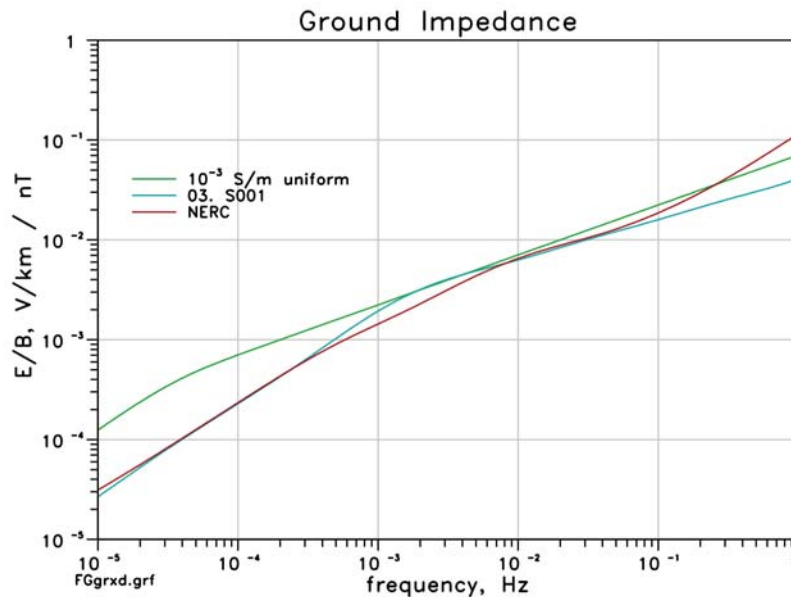


Figure 6 Ground profile B-to-E conversion in the frequency domain for three cases.

conductivity level that continues downward at its last value.<sup>10</sup> The E3 HEMP heave signals (due to their low frequency content) can penetrate through the upper layers of the Earth but will not penetrate much deeper when they encounter a high conductivity lower level (due to the pressures and temperatures found in the upper mantle of the Earth). The blue line is another set of ground conductivity data applicable to eastern Canada developed by Metatech from geological data. The impedance curve developed from this conductivity profile is seen to be very similar to the NERC curve in Figure 6. The third profile shown (in green) has a uniform conductivity of  $10^{-3}$  S/m, which is used for simplicity in the E3 HEMP heave simulations shown later in this report.

Figure 6 shows the resulting impedance (conversion of B to E) in the frequency domain. There are many ways to deal with these types of impedance curves relating E to B, although the technique used by the authors allows calculations of E from B in the time domain without converting to the frequency domain.<sup>11</sup> This has advantages for performing real-time computations when measuring geomagnetic storm disturbances. All three curves are reasonably close together for the important frequency range of 1 to 100 mHz, as this is the frequency range of typical E3 HEMP B-field disturbances.

<sup>10</sup> "Transmission System Planned Performance for Geomagnetic Disturbance Events", TPL-007-1, available at <https://bit.ly/2GQpQF1>

<sup>11</sup> J.L. Gilbert, W.A. Radasky and E.B. Savage, "A Technique for Calculating the Currents Induced by Geomagnetic Storms on Large High Voltage Power Grids," IEEE EMC Symposium, Pittsburgh, August 2012, pp. 323-328.

### 3 SOVIET E3 HEMP MEASUREMENTS

Toward the end of the development of the E3 HEMP computational models in the U.S., a paper that reported measurements made by the Soviet Union during two of their high-altitude nuclear tests in 1962 was provided to us through the U.S. Congressional EMP Commission by Soviet scientists.<sup>12</sup> This was high quality data, in that measurements were made at three fixed locations (designated N1, N2, and N3 by the Soviets as shown in Table 1 and Figure 7), and the B field measurements were provided for two horizontal vector components. There is some uncertainty concerning the precision of the test and measurement locations; however, the data provided greatly increased the information describing the E3 HEMP heave signal. High-altitude nuclear tests were performed by the U.S. mainly over the Pacific Ocean, and the locations for measuring the magnetic fields were not as diverse as for the Soviet measurements.

#### TEST PARAMETERS

The Soviet tests were reported to be at burst heights of 150 and 300 km altitudes, for the same device design with an estimated yield of 300 kT. The precise geometry (burst and observer locations) is not known, as there was some ambiguity in the data provided. The Soviet measurement paper does give range values (burst to observer distances) for all six measurements (three from each test), and these same values appear elsewhere in a consistent manner. (The Soviets tended to use the slant range from the burst to the ground location, not the ground range, but the ground range is easily calculated from the burst height.) A set of locations was used that are consistent with these values in the following discussions, using the understanding of the variation of the fields with location. These burst and observer locations are given in Table 1.

*Table 1 Geometry for the Soviet High-Altitude Tests.*

Test Locations			
Type	Position	Latitude (N)	Longitude (E)
Bursts	R1, 300 km	47.6°	64.9°
	R2, 150 km	47.0°	68.0°
Observers	N1	47.9°	67.4°
	N2	47.1°	70.6°
	N3	45.9°	72.1°

<sup>12</sup> "Characteristics of magnetic signals detected on the ground during the Soviet nuclear high-altitude explosions," memorandum provided by Soviet scientists, February 2003.

Using the simulation code in Meta R-321, the B field peak values were calculated for the two burst heights. The data is shown in Figure 7 for the 150 km burst height (R1) and in Figure 8 for 300 km (R2).<sup>13</sup> (The 300 km test was actually performed 6 days before the 150 km test, but the lower altitude case was described first). The peak contours are identified by their color, and the B field directions at the time of the peak are shown by the arrows. The burst and observer points are marked on the displays. Normalized results are shown in these figures as a nominal contour plot is desired to be used later in this report as a standard contour profile.

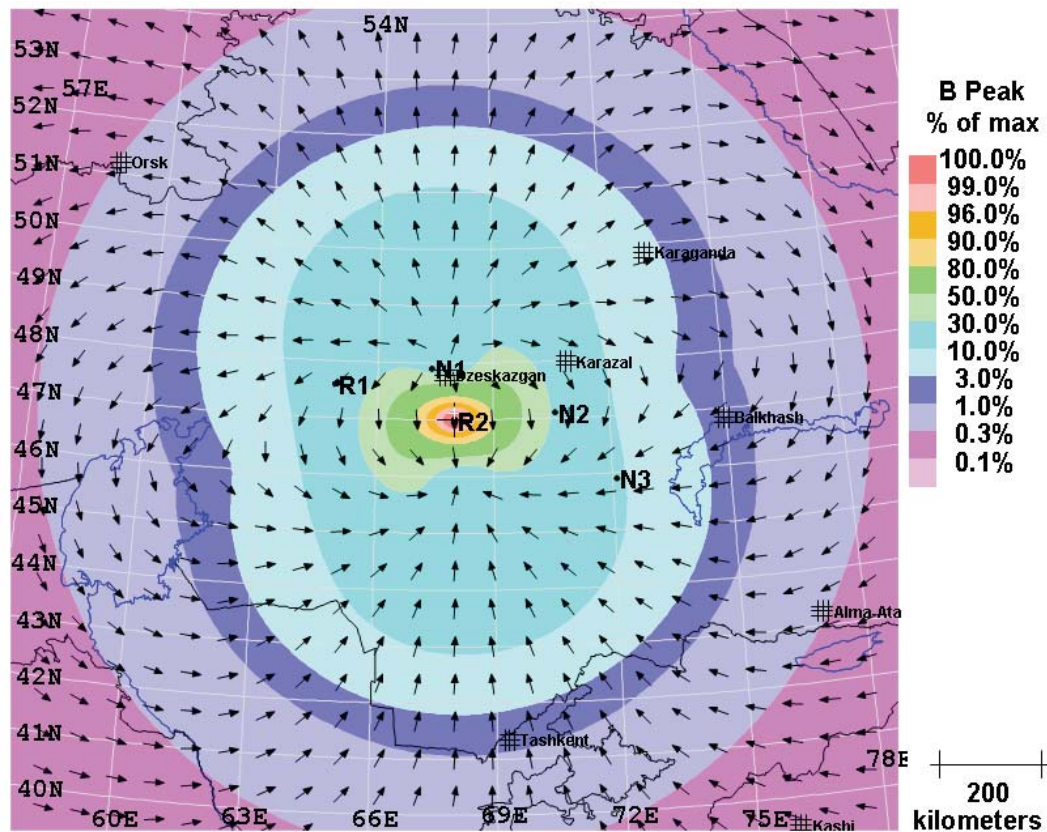


Figure 7 Simulation of the Soviet tests showing B field peaks and field directions, 150 km test (R2).

<sup>13</sup> J.L. Gilbert, W.A. Radasky, K.S. Smith, K. Mallen, M.L. Sloan, J.R. Thompson, C.S. Kueny and E. Savage, "HEMPTAPS/HEMP-PC Audit Report." Meta R-131, December 1999; DTRA-TR-00-1, April 2002.



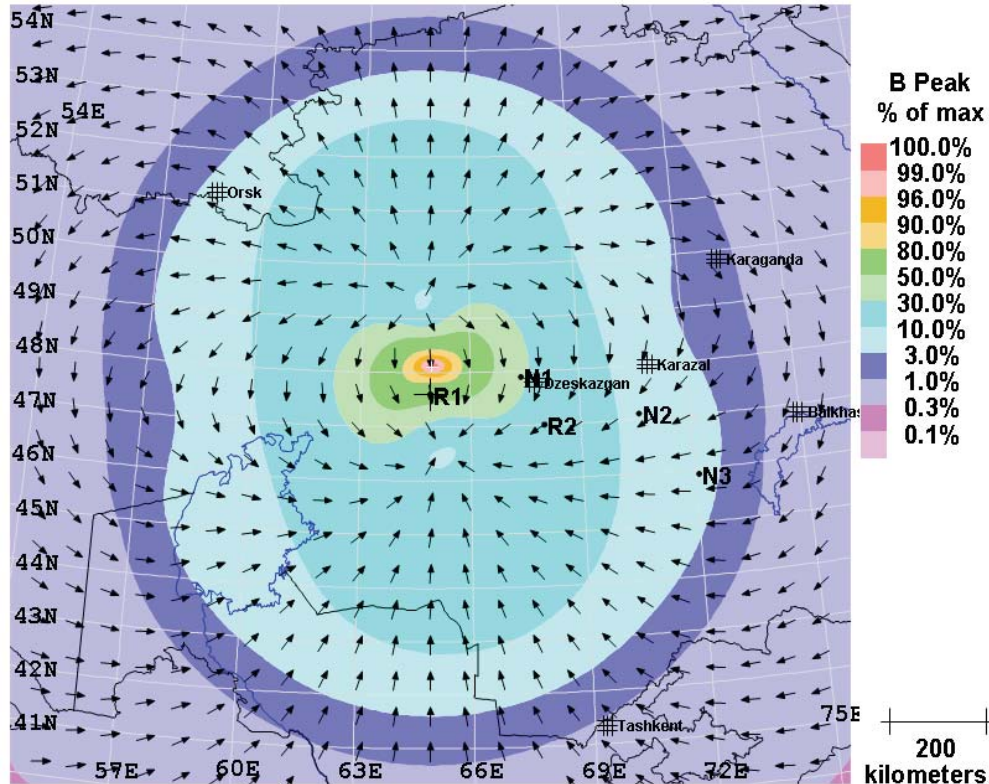


Figure 8 Simulation of the Soviet tests showing B field peaks and field directions, 300 km test (R1).

The next set of figures shows the measured B field time waveforms. The three lines are the north and west components, and the resulting magnitude. For the 150 km burst height case, shown in Figure 9 to Figure 11, the waveforms are all relatively wide in pulse width (the N1 case waveform has not returned to zero at the end of the 100-second window of the measurements). The peak occurs between times of 35 to 70 seconds. Figure 7 shows that N1 is close to the northern area of the two electric field depression points (the locations around which the two loops of E field circulate, as seen earlier in Figure 2) for this case. Here the time waveform may be complicated due to some shifting with time of the field depression point position. For the 300 km burst height waveforms, Figure 12 to Figure 14, the signals are faster, especially for N1. As noted, faster rising waveforms for the B fields enhance the E fields, because the impedance of the Earth behaves as  $f^{-1/2}$  ( $f$  = frequency) as shown in Figure 6.



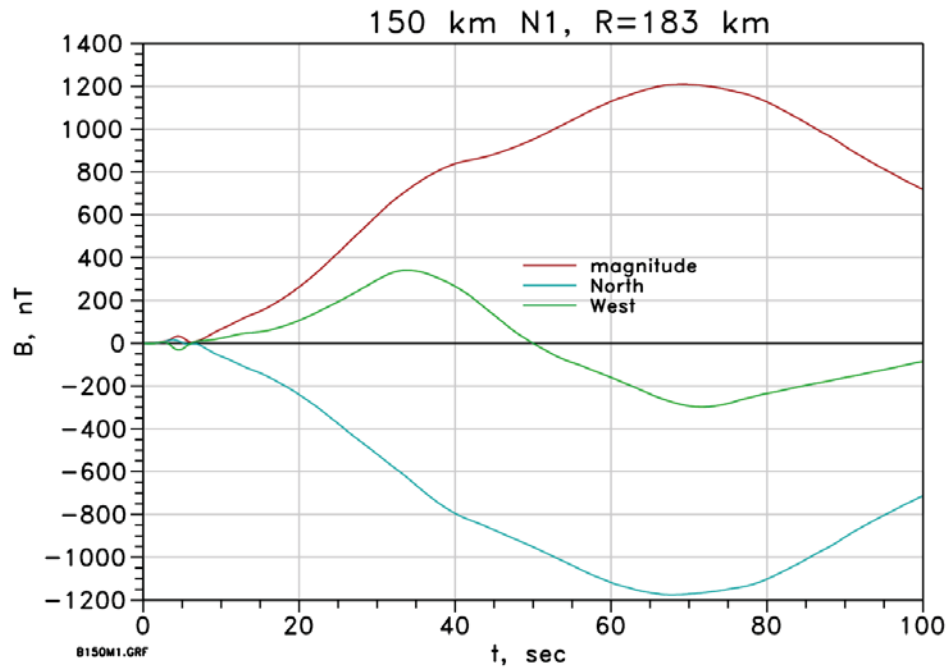


Figure 9 Measured B fields at N1, 150 km test.

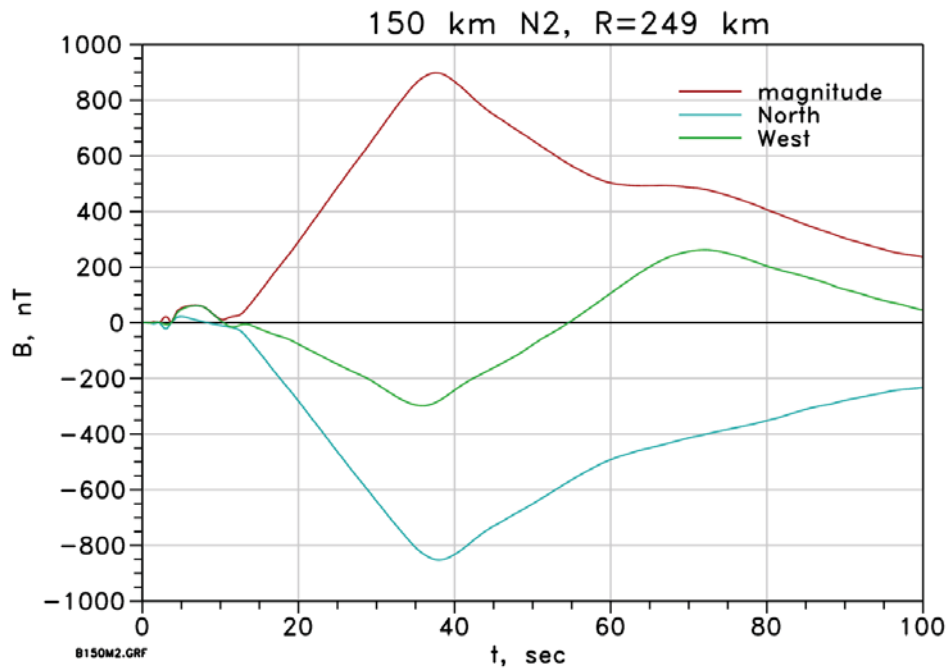


Figure 10 Measured B fields at N2, 150 km test.

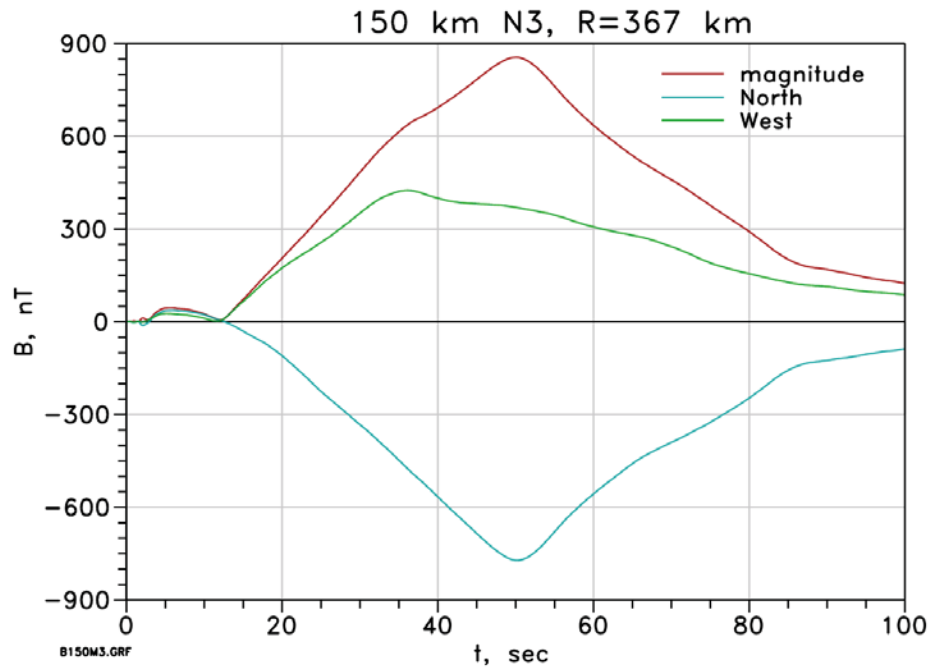


Figure 11 Measured  $B$  fields at N3, 150 km test.

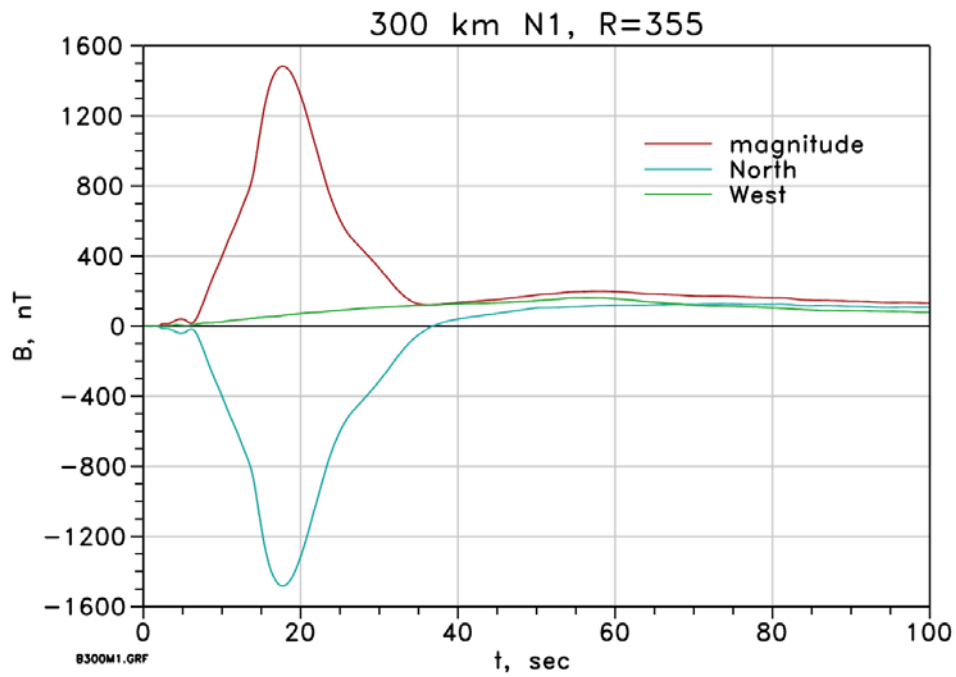


Figure 12 Measured  $B$  fields at N1, 300 km test.

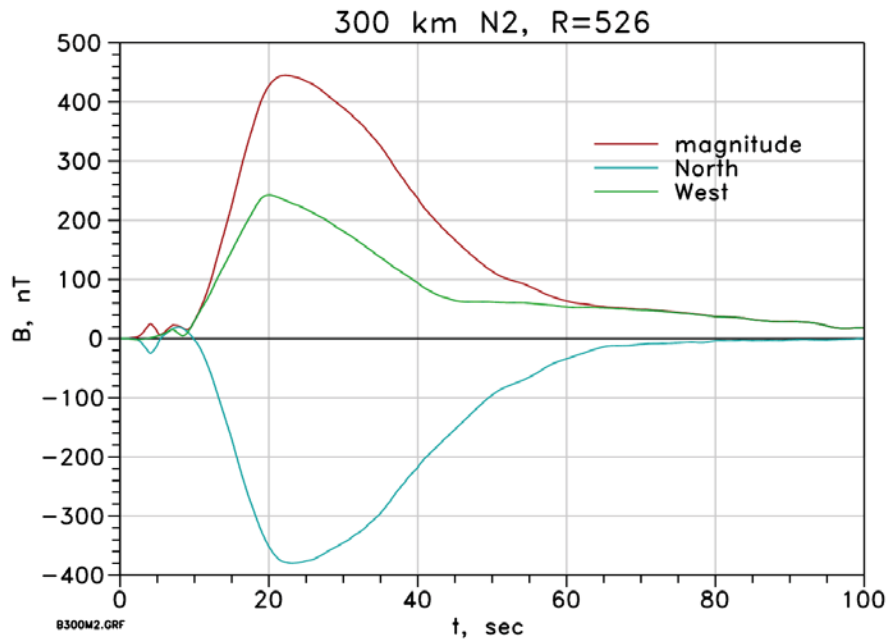


Figure 13 Measured B fields at N2, 300 km test.

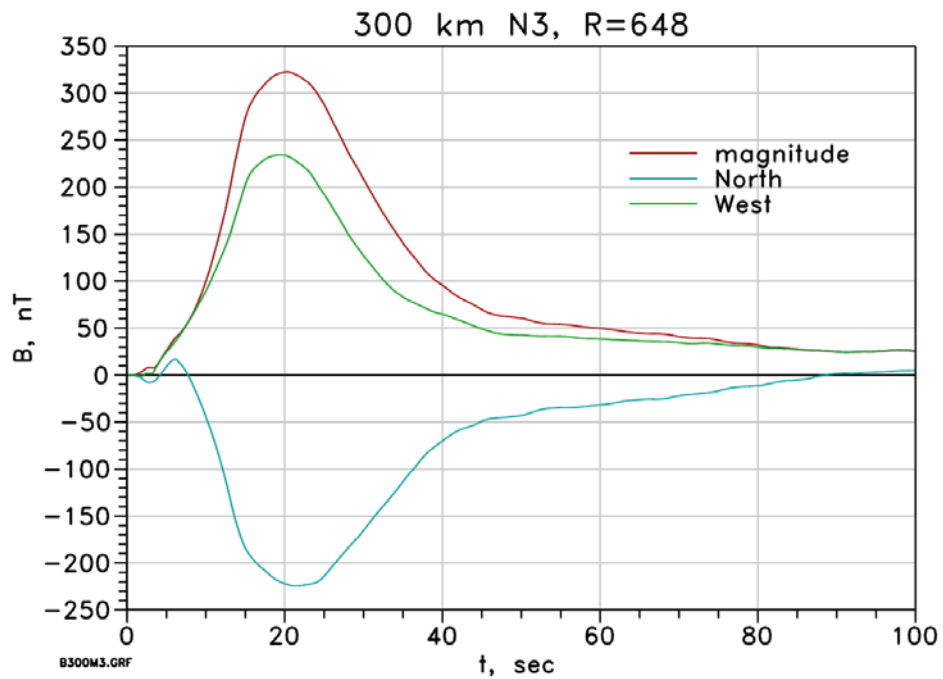


Figure 14 Measured B fields at N3, 300 km test.

The electric fields are now calculated from the measured B fields, given in nanoTeslas (nT). Table 2 lists the peak values for the calculated E fields, along with the peak values for the measured B and B-dot. The time derivative of B is often a good proxy for the behavior of the peak value of the electric field for a given ground conductivity profile. That is to say that for a given profile increases in the time derivative of the B field result in higher peak electric fields. It is noted, however, that the rest of the computed time waveform of the electric field depends more on the shape of the impedance curve and using the time derivative of the B field to compute the entire electric field waveform will not result in an accurate E field waveform.

For the following plots the measured B field components were individually computed for four sample ground profiles (a fourth severe ground profile and impedance curve was added to the previous set of three), and the resulting E field magnitudes are plotted (the total horizontal electric field is calculated by separately calculating the electric fields from the two orthogonal B field components). The 150 km cases are presented in Figure 15 to Figure 17, and the 300 km cases are presented in Figure 18 to Figure 20. These show that E fields are similar for the three ground profiles described in Figure 6. Further, the dark blue line shows the E field for a ground profile that has a very low conductivity. This profile was developed for southern Sweden and has also been used for a limited region in the northeastern United States, but it has not been used to develop the E3 HEMP results here. It is presented only to indicate that large electric fields are possible in some locations.

The highest computed E fields are for the N1 observer for the 300 km burst case. This had the highest measured B fields, and also had the narrowest time waveform—the computed peak E fields are driven higher by the enhanced time derivative of the B.

*Table 2 Peaks of the Soviet measurement waveforms. (The E field is for the  $10^{-3}$  S/m ground.)*

Measurement Peaks				
Burst	Observer	Peaks		
		B, nT	$\dot{B}$ , nT/min	E, V/km
R2 150 km	N1	1208.99	2141.2	4.885
	N2	898.27	3526.3	5.580
	N3	856.08	2240.2	4.241
R1 300 km	N1	1484.05	17581.4	16.585
	N2	444.69	3064.8	4.110
	N3	322.57	2642.9	3.113

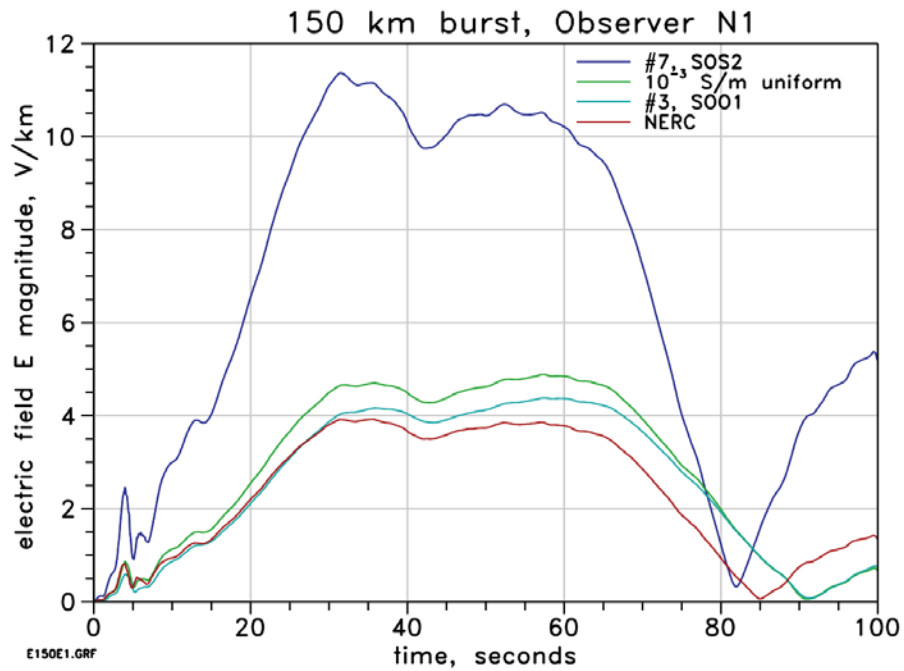


Figure 15 E field amplitudes for four ground profiles, at N1, 150 km test.

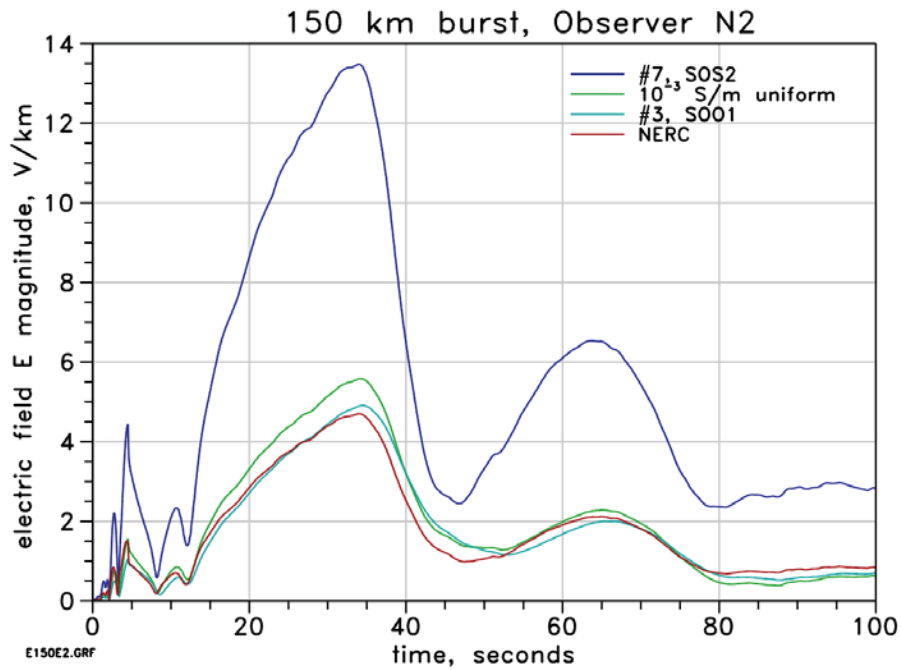


Figure 16 E field amplitudes for four ground profiles, at N2, 150 km test.

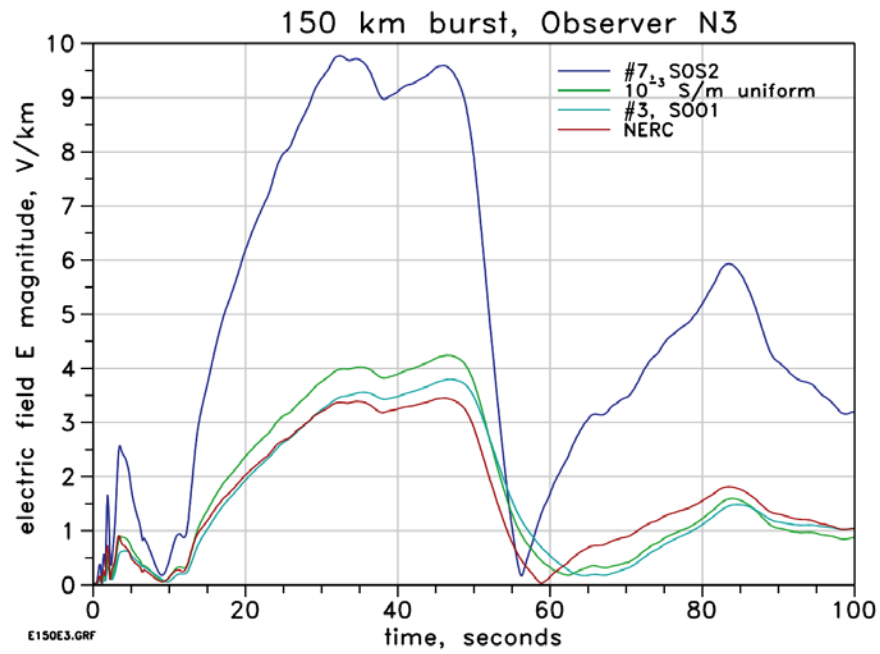


Figure 17 E field amplitudes for four ground profiles, at N3, 150 km test.

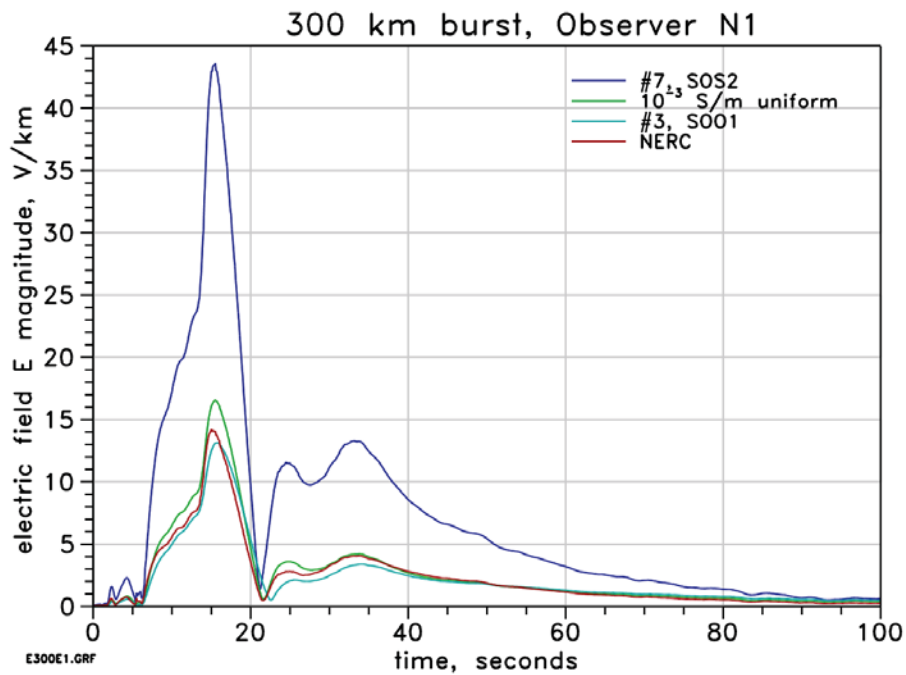


Figure 18 E field amplitudes for four ground profiles, at N1, 300 km test.



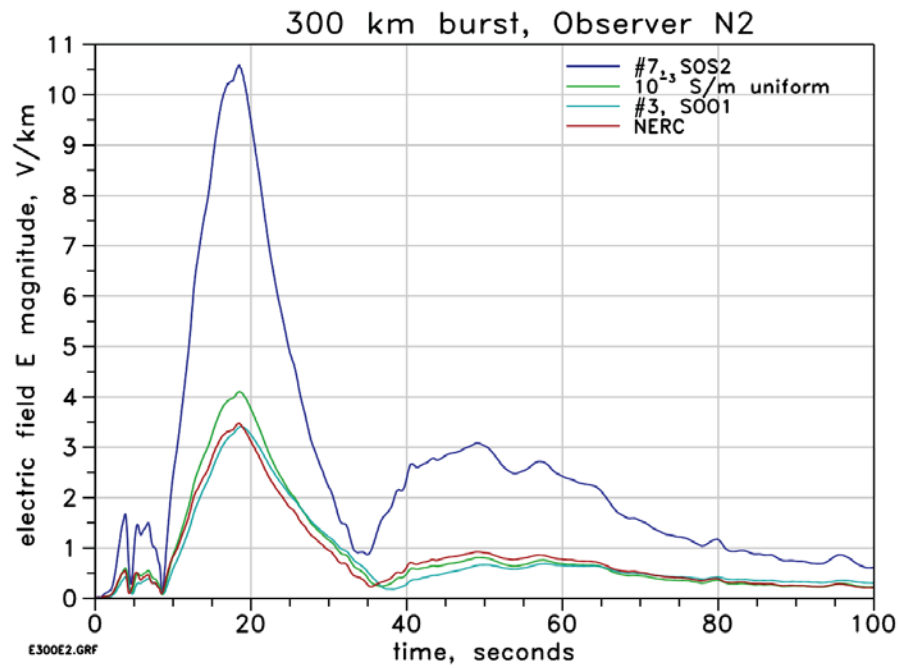


Figure 19 E field amplitudes for four ground profiles, at N2, 300 km test.

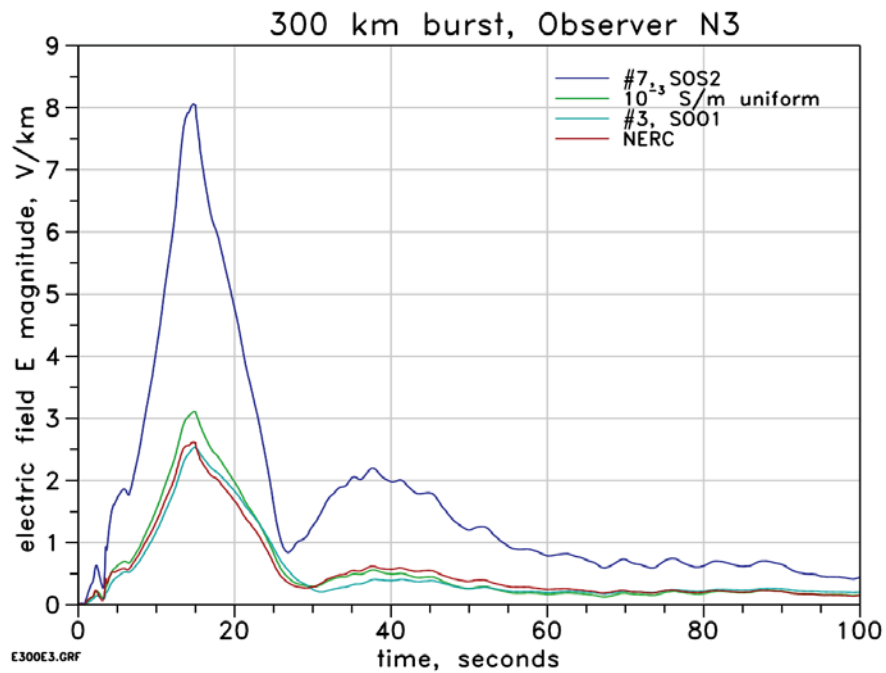


Figure 20 E field amplitudes for four ground profiles, at N3, 300 km test.

## SCALING OF THE RESULTS

Even at this date the calculational models of E3 HEMP heave are not considered to be perfect, and therefore measurements are the most believable evidence of possible E3 HEMP heave field levels. However, it is extremely unlikely that even these few high-quality measurements captured the highest peak fields. Of course other test devices, especially with higher yields, could have produced higher fields, and there can be vast variations in the atmosphere conditions. For this report, the parameters of interest are the locations of the measurement observers and of the burst itself. Specific parameters are the impacts due to the geomagnetic latitude of the bursts, and whether a better location exists to place measurement sites relative to each burst. The first question is: how much higher could the measured fields have been if the burst location were closer to the geomagnetic equator? The second question is because the fields were measured at only three locations, none of which were likely to have been at the optimum point, can the measurements be scaled to the optimum point?

## LATITUDE SCALING

The first consideration is the geomagnetic latitude. The geomagnetic latitude values for the two cases are found from the given physical locations:

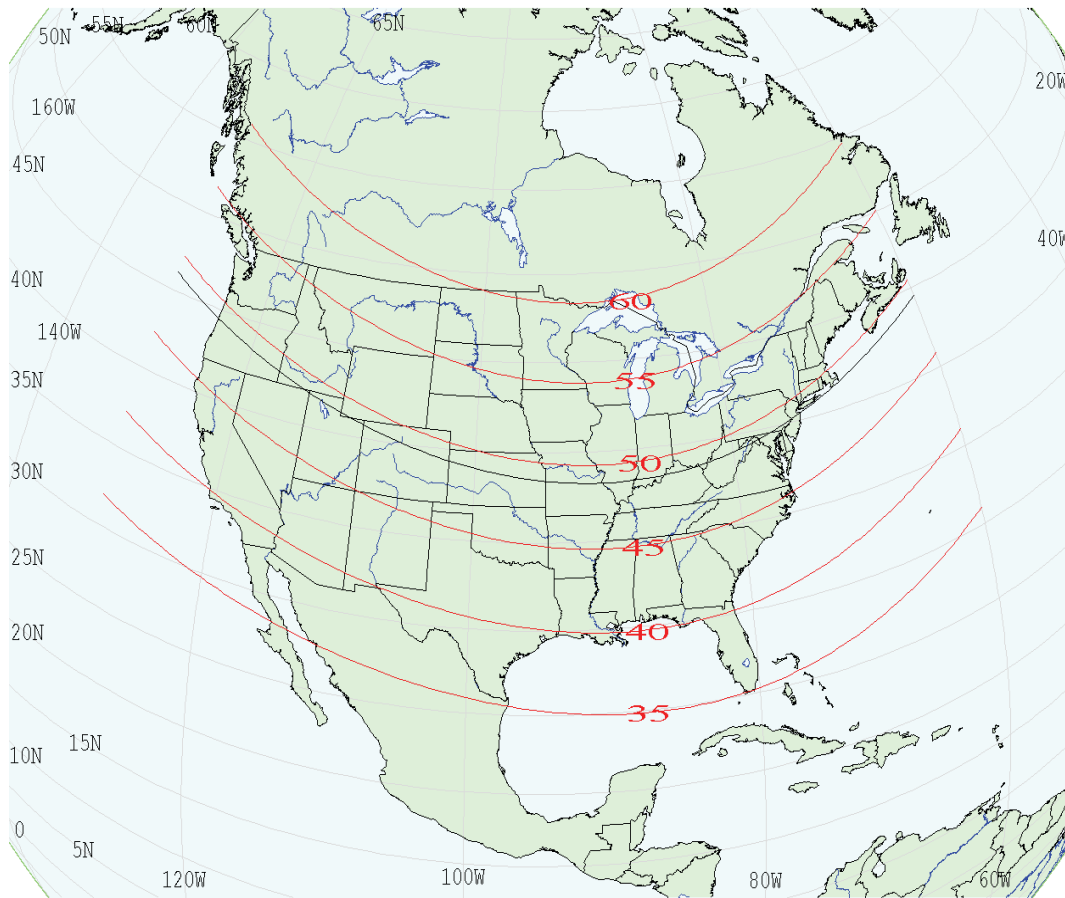
150 km: 48.92° N

300 km: 46.13° N

These values depend on knowing the burst locations, for which there is some uncertainty, but the precise values were likely within a few degrees of these values. As discussed, the maximum peak magnetic fields increase for lower geomagnetic latitudes per the basic models.

Considering the 150 km burst case, Figure 21 shows the equivalent locations for the continental U.S. The marked red lines show geomagnetic latitude lines, and there is a black line for the 48.92°N magnetic latitude corresponding to the 150 km HOB Soviet test. If the burst had been placed anywhere along this line, the maximum peak B fields would have been as in the Soviet test. For bursts below (south) this black line, the fields would be higher.

The map shows that Texas and Florida can be as low as 35°N geomagnetic latitude. The simulation code used to perform the calculations was the same as used for the simulations shown in Figure 7 and Figure 8, but with the burst moved to lower geomagnetic latitudes—specifically the cases of 35°N that correspond to the southern points for Florida and Texas, and also for the highest levels worldwide (the geomagnetic equator). Next, the ratios of the maximum B fields from these simulations at other latitudes were compared to the maximum values for the Soviet measurement location, to get the results shown in Table 3. Using these ratio values, the Soviet measurements (“Soviet” column) were scaled to the corresponding maxima for the other latitude burst locations.



*Figure 21 Geomagnetic latitude variation, for a 150 km burst, over the U.S. The black line is at 48.92°, which is the computed geomagnetic latitude for the 150 km Soviet test.*

Locations outside of the continental U.S. include both lower and higher geomagnetic latitudes. The table therefore includes scaling for a magnetic latitude of 22° N, which is appropriate for Oahu, Hawaii, and also for a magnetic latitude of 65° N, as would apply to Fort Greely, Alaska.

## PATTERN SCALING

The burst locations were different for the two tests, but the three observer locations stayed the same for the two tests. There is some uncertainty, however, in both the burst points and observer points. However, it is likely that the fields were higher at locations other than the three places that happened to be selected for the measurement sites. Here some understanding is sought for how high the measured fields might have been if there was a measurement at the optimal location. Figure 7 (the 150 km case), for example, shows that for this HOB the maximum is close to being directly under the burst, but the measurement sites were further out.

Table 3 Geomagnetic latitude scaling of the Soviet measurements.

Scaling of Measurements to Other Magnetic Latitudes								
Burst (km)	Observer	Burst Locations						
		Soviet, B, nT	Alaska, 65° N		U.S., 35° N		Hawaii, 22° N	
			Scaling factor	B, nT	Scaling factor	B, nT	Scaling factor	B, nT
R2 150	N1	1208.99	0.600	725.28	1.364	1648.65	1.675	2025.50
	N2	898.27		538.88		1224.93		1504.93
	N3	856.08		513.56		1167.40		1434.24
R1 300	N1	1484.05	0.577	855.62	1.274	1890.47	1.537	2280.36
	N2	444.69		256.38		566.47		683.29
	N3	322.57		185.98		410.91		495.66

As noted, there is some uncertainty in the modeling and for the model parameters to use to simulate the Soviet tests. Good confidence exists, however, in the values for the ranges to the measurement sites. With this in mind, the simulation shown in Figure 22 performs E3 HEMP heave calculations at points on a 2D polar mesh; for each range of this mesh all the azimuth angles were searched to obtain three norm values: maximum, average, and minimum. The overall maximum was identified and the three norm values were normalized to this maximum value, to obtain the three lines in the plot.

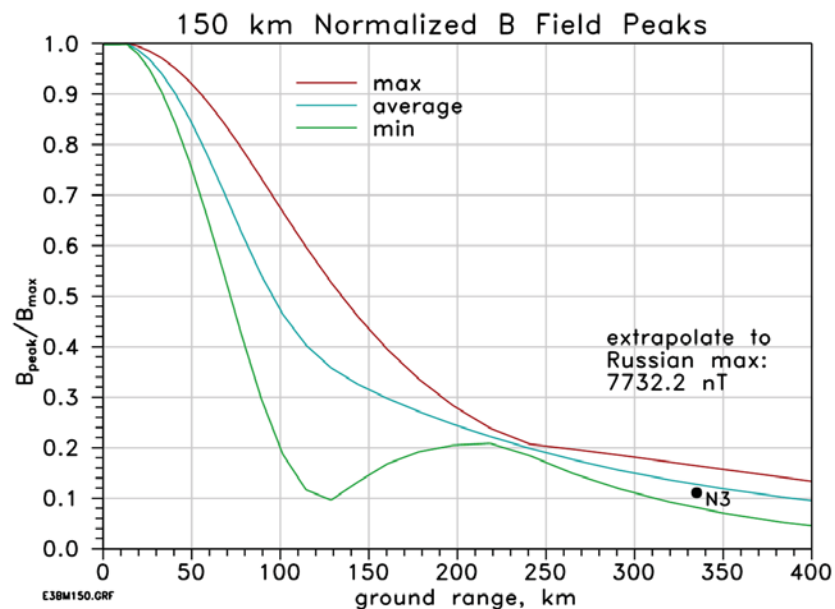


Figure 22 Normalized simulated B field peaks versus ground range for the 150 km test. The black dot

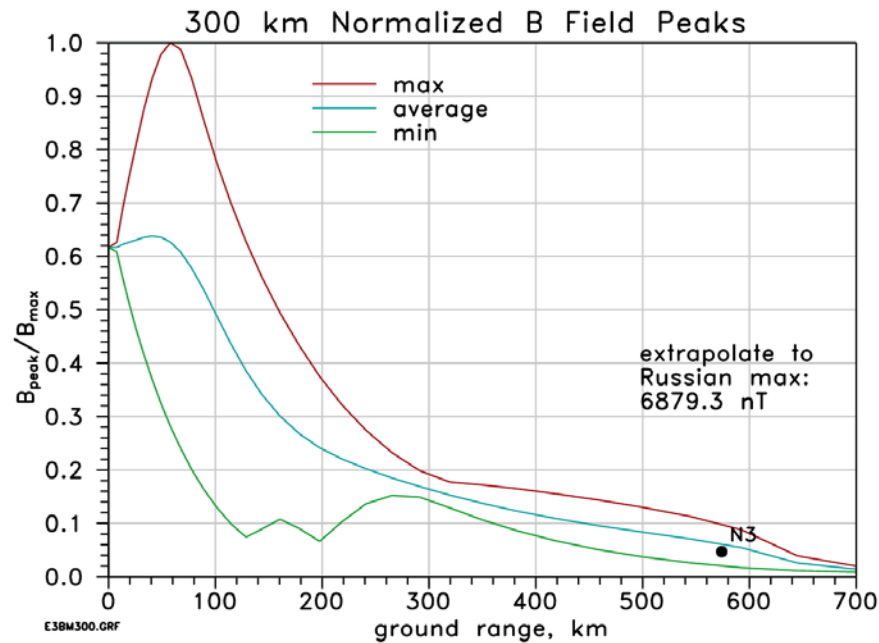


Figure 23 Normalized simulated B field peaks versus ground range for the 300 km test. The black dot shows the simulated results for the N3 point.

As noted, the precise observer azimuth positions are unknown, but the normalized value for the assumed position of the N3 observer is shown (the black dot) using a best-estimate location. Note that at this range there is not as much structure to the azimuth variation as there is closer in, such as at the 120 km range, so there is less uncertainty associated with the exact azimuth position for N3. Another way of stating this is to observe that the contour pattern becomes more circular as the observer is further away from surface zero. Using this pattern, the estimate for the maximum is then given by scaling with the factor of 9.03 ( $1/0.111$ ) from the N3 point to the optimum position. The same method was used for the 300 km burst height, in the plot shown in Figure 23.

Table 4 summarizes the scaling for the two cases. The scaled values are listed in the last column. These are found by multiplying the N3 measurements (the 3<sup>rd</sup> column) by the scaling

Table 4 Pattern (observer position) scaling of the Soviet measurements.

Scaling from N3 up to the Maximum Point				
Case	Soviet Measurements		Scaling	
	N1, B (nT)	N3, B (nT)	Scaling Factor	Max, B (nT)
R2, 150 km	1209.0	856.08	9.03	7732.2
R1, 300 km	1484.0	322.57	21.33	6879.3

factors (4<sup>th</sup> column, given by the reciprocal of the N3 values in Figure 22 and Figure 23). For comparison, the maximum measured values are listed in the 2<sup>nd</sup> column (the N1 points). The fact that these are smaller than the scaled maximum values is an indication that none of the observer points were very close to the optimum position.



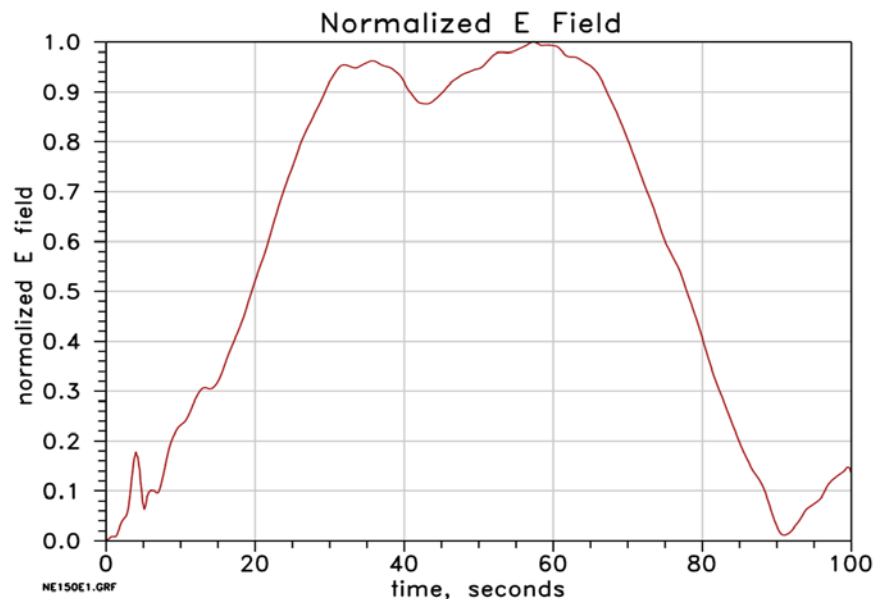
## 4 CONCLUSIONS

The Soviet measurements of the E3 HEMP heave B fields were converted to E fields for a reasonable bounding case of a uniform ground conductivity of 1 mS/m. None of the three measurement points of the E3 HEMP heave fields were near the maximum in the expected field pattern, and column 3 in Table 5 gives estimates of the scaling of the measurements to the expected maximum. The three right columns provide the scaling for magnetic latitude to Hawaii, the southern portion of the continental United States, and Alaska.

*Table 5 Scaling of the Soviet Measurements.*

<b>Scaling from N3 up to the Maximum Point, for Three Latitudes for <math>10^{-3}</math> S/m</b>					
Case	Soviet Measurements		Latitude Scaling, E, V/km		
	Latitude (N)	E, V/km	22° N	35° N	65° N
R2, 150 km	48.92°	38.31	64.18	52.24	22.98
R1, 300 km	49.10°	66.39	102.02	84.57	38.28

Figure 24 provides a normalized waveform for one of the E fields. The electric field waveform can be used when computing the induced currents flowing in power lines, for example, to determine the amount of heating in transformer hot spots, as the time dependence of the currents are important in determining thermal effects. Figure 25 provides a sample normalized ground pattern, showing the spatial fall-off from the maximum value. Note that



*Figure 24 E field waveform shape, using the measured N1 waveform from the 150 km burst height*

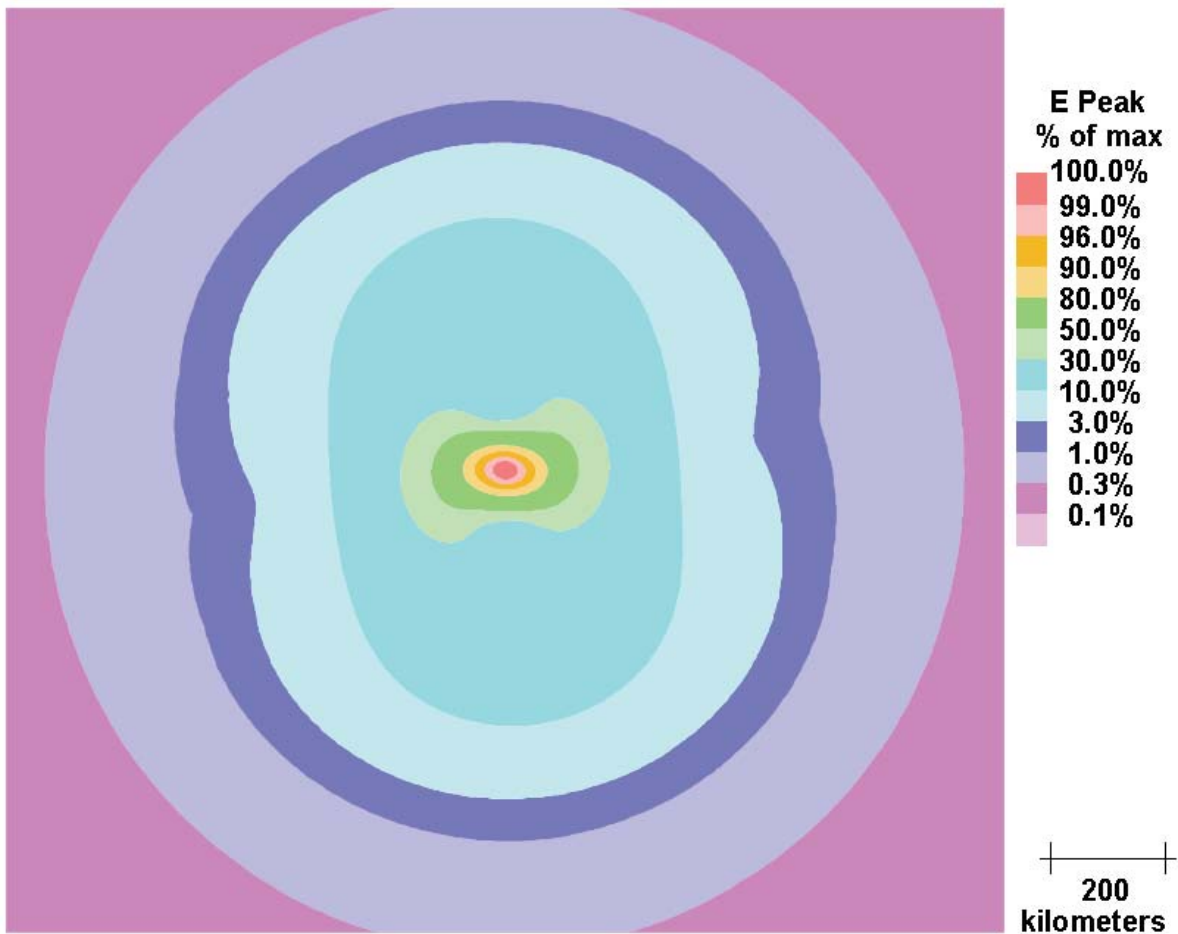


Figure 25 Normalized E peak contour pattern from the 150 km burst case

higher yield bursts could lead to even higher maximum fields, although as shown in the generic curve in Figure 3, the peak value tends to saturate as yields increase. However, this is not true for area coverage, as increasing to larger yields can increase the spatial extent of the high field region.

From: [Joseph McClelland](#)  
To: (b) (6)  
Subject: FW: EMP COMMISSION REPORTS  
Date: Wednesday, May 09, 2018 4:56:00 AM  
Attachments: [Executive Report on Assessing the Threat from EMP - FINAL April2018.pdf](#)  
[Recommended E3 Waveform for Critical Infrastructures - FINAL April2018.pdf](#)  
[Life Without Electricity - FINAL April2018.pdf](#)  
[EMP Commission Vol1 Summary.pdf](#)  
[EMP COMM. RPT. CRIT. NAT. INFRASTRUCTURES.pdf](#)

---

Hi (b) (6),  
Please print in color.  
Thanks,  
Joe

---

**From:** Peter Pry [mailto:peterpry@verizon.net]  
**Sent:** Wednesday, May 09, 2018 12:33 AM  
**To:** Joseph McClelland <Joseph.McClelland@ferc.gov>  
**Subject:** EMP COMMISSION REPORTS

Attached find the 3 unclassified 2018 EMP Commission reports and the two unclassified 2004 and 2008 EMP Commission Reports. 7 more EMP Commission reports, submitted to DOD unclassified that were supposed to be published in December 2017, still undergoing review (or being stalled) by DOD.--Peter

Dr. Peter Vincent Pry  
Executive Director  
EMP Task Force on National and Homeland Security  
Former Chief of Staff  
Congressional EMP Commission

# Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

*Critical National Infrastructures*





# Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

## *Critical National Infrastructures*

### **Commission Members**

Dr. John S. Foster, Jr.

Mr. Earl Gjelde

Dr. William R. Graham (Chairman)

Dr. Robert J. Hermann

Mr. Henry (Hank) M. Kluepfel

Gen Richard L. Lawson, USAF (Ret.)

Dr. Gordon K. Soper

Dr. Lowell L. Wood, Jr.

Dr. Joan B. Woodard

**April 2008**





## Table of Contents

	<u>Page</u>
<b>Preface.....</b>	<b>vi</b>
<b>Acknowledgements .....</b>	<b>ix</b>
<b>Chapter 1. Infrastructure Commonalities.....</b>	<b>1</b>
SCADA Systems.....	1
Impact of SCADA Vulnerabilities on Critical Infrastructures: Historical Insight.....	6
Infrastructures and Their Interdependencies.....	9
Commission-Sponsored Modeling and Simulation (M&S) Activities .....	13
Summary .....	15
Recommendations.....	16
<b>Chapter 2. Electric Power .....</b>	<b>17</b>
Introduction.....	17
Description.....	20
Vulnerabilities.....	29
Test Results.....	37
Historical Insights .....	41
Distinctions .....	43
Strategy .....	45
Recommendations.....	53
<b>Chapter 3. Telecommunications.....</b>	<b>62</b>
Introduction.....	62
Telecommunications Support During Emergencies .....	64
EMP Impact on Telecommunications.....	65
Recommendations.....	79
<b>Chapter 4. Banking and Finance.....</b>	<b>83</b>
Introduction.....	83
The Financial Services Industry.....	85
Vulnerability to EMP .....	88
Consequences of Financial Infrastructure Failure .....	92
Recommendations.....	94
<b>Chapter 5. Petroleum and Natural Gas .....</b>	<b>95</b>
Introduction.....	95
Infrastructure Description .....	95
Direct Effects of EMP on Petroleum and Natural Gas Infrastructure.....	98
Petroleum Infrastructure and SCADA .....	98
Natural Gas Infrastructure and SCADA .....	99
Effects of an EMP Event on the U.S. Petroleum and Natural Gas Infrastructures.....	100
Indirect Effects of EMP: Accounting for Infrastructure Interdependencies .....	102
Recommendations.....	103
<b>Chapter 6. Transportation Infrastructure .....</b>	<b>105</b>
Introduction.....	105
Long-Haul Railroad .....	106
The Automobile and Trucking Infrastructures.....	112
Maritime Shipping .....	116

Commercial Aviation.....	122
Recommendations.....	127
<b>Chapter 7. Food Infrastructure.....</b>	<b>129</b>
Introduction.....	129
Dependence of Food on Other Infrastructures.....	129
Making, Processing, and Distributing Food.....	130
Vulnerability to EMP.....	132
Consequences of Food Infrastructure Failure.....	134
Recommendations.....	137
<b>Chapter 8. Water Infrastructure.....</b>	<b>139</b>
Introduction.....	139
The Water Works.....	140
Vulnerability to EMP.....	142
Consequences of Water Infrastructure Failure.....	143
Recommendations.....	146
<b>Chapter 9. Emergency Services.....</b>	<b>147</b>
Introduction.....	147
Emergency Services Systems Architecture and Operations.....	147
Impact of an EMP Attack.....	149
Recommendations.....	156
<b>Chapter 10. Space Systems.....</b>	<b>158</b>
Introduction.....	158
Terms of Reference for Satellites.....	159
Line-of-Sight Exposure to a Nuclear Detonation.....	159
Persistently Trapped Radiation and Its Effects.....	161
Nuclear Weapon Effects on Electronic Systems.....	162
Satellite Ground Stations.....	167
Discussion of Results.....	168
Findings.....	170
Recommendations.....	171
<b>Chapter 11. Government.....</b>	<b>172</b>
Introduction.....	172
Maintaining Government Connectivity and Coherence.....	172
Recommendations.....	172
<b>Chapter 12. Keeping The Citizenry Informed: Effects On People.....</b>	<b>176</b>
Introduction.....	176
Impact of an EMP Attack.....	176
Recommendations.....	181
<b>Appendix A. The Commission and Its Charter.....</b>	<b>A-1</b>
Organization.....	A-1
Method.....	A-2
Activities.....	A-2
<b>Appendix B. Biographies.....</b>	<b>B-1</b>

## List of Figures

	<u>Page</u>
Figure 1-1. Typical SCADA Architecture .....	2
Figure 1-2. Generic SCADA Architecture.....	3
Figure 1-3. PLC Switch Actuator .....	4
Figure 1-4. EMP Simulator with Test Structures and Internal Electronics .....	5
Figure 1-5. Some of the Electronic Control Systems Exposed in Test Facility .....	6
Figure 1-6. Physical Model Used to Quantify Coupling to Different Cable Lengths in a Hypothetical Local Area Network (LAN) .....	7
Figure 1-7. A Conceptual Illustration of the Interconnectedness of Elements Contained Within Each Critical Infrastructure. ....	12
Figure 1-8. Interdependency for Anticipated Network of the Future .....	14
Figure 1-9. Results of a Model Simulation .....	15
Figure 2-1. Power System Overview .....	21
Figure 2-2. NERC Interconnections .....	25
Figure 2-3. GIC Damage to Transformer During 1989 Geomagnetic Storm .....	33
Figure 2-4. EMP Simulator.....	38
Figure 2-5. Test Item: Electronic Relay.....	40
Figure 2-6. Flashover Observed During Injection Pulse Testing .....	41
Figure 3-1. Generic Telecommunications Network Architecture.....	66
Figure 3-2. September 11, 2001, Blocked Call Rate—Cellular Networks .....	70
Figure 3-3. Example Network Management Facility .....	71
Figure 3-4. Cellular Base Station Equipment .....	72
Figure 3-5. Routers Collecting Network Management Data .....	72
Figure 3-6. Cellular Network Testing at INL .....	74
Figure 3-7. Testing at NOTES Facility.....	74
Figure 3-8. Secure Access Card and Cell Phones.....	75
Figure 3-9. Percentage of Calls Completed Immediately After EMP Event.....	76
Figure 3-10. Percentage of Calls Completed 4 Hours After EMP Event .....	76
Figure 3-11. Percentage of Calls Completed 2 Days After EMP Event.....	77
Figure 3-12. Percentage of Calls Completed at Time T (Logarithmic Time Scale) (Within EMP Contours).....	77
Figure 5-1. Petroleum Infrastructure.....	96
Figure 5-2. Natural Gas Infrastructure.....	97
Figure 5-3. Typical SCADA Arrangement for Oil Operations.....	99
Figure 5-4. SCADA Integrates Control of Remote Natural Gas Facilities.....	100
Figure 5-5. Examples of Oil Interdependencies .....	102
Figure 5-6. Examples of Natural Gas Interdependencies .....	102
Figure 6-1. 2003 Class I Railroad Tons Originated.....	107
Figure 6-2. CSXT Train Dispatch Center .....	108
Figure 6-3. Typical Block Signal Control Equipment Enclosure .....	110
Figure 6-4. Grade Crossing Shelter and Sensor Connection .....	110
Figure 6-5. Modern Locomotive Functional Block Diagram .....	111
Figure 6-6. A Typical Signalized Intersection.....	113
Figure 6-7. Container Cranes and Stored Containers .....	117
Figure 6-8. RTG at Seagirt Marine Terminal .....	118
Figure 6-9. Handheld Wireless Data Unit.....	119

Figure 6-10. Truck Control Station.....	119
Figure 6-11. An ARTCC Operations Room .....	122
Figure 9-1. A Generic Modern Emergency Services System .....	148
Figure 10-1. From left to right, the ORANGE, TEAK, KINGFISH, CHECKMATE, and STARFISH high-altitude nuclear tests conducted in 1958 and 1962 by the United States near Johnston Island in the mid- Pacific .....	159
Figure 10-2. Satellite Orbits Illustrated .....	159
Figure 10-3. Areas of Space Irradiated by Photons and Neutrons.....	160
Figure 10-4. Naturally occurring belts (Van Allen belts) of energetic particles persistently trapped in the geomagnetic field are illustrated .....	161
Figure 10-5. Schematic diagram of relative intensities of trapped fluxes from two identical high-altitude nuclear detonations .....	161
Figure 10-6. Satellites remaining after a 10 MT burst over Lake Superior .....	167
Figure 10-7. Satellite ground-based receiver outage time after a 10 MT burst over Lake Superior.....	167
Figure 10-8. HEO satellite exposure to trapped radiation produced by Events 11, 17, and 21 .....	168

### List of Tables

Table 3-1. Telecommunications Equipment Tested .....	73
Table 10-1. Trial Nuclear Events.....	163
Table 10-2. Analysis of Satellites .....	164
Table 10-3. Probability That Satellites Suffer Damage by Direct Exposure to X-Rays .....	165
Table 10-4. Trial Events in Group 1 .....	165
Table 10-5. Trial Events in Group 2 .....	166
Table 10-6. Trial Events in Group 3 .....	166

## Preface

The physical and social fabric of the United States is sustained by a system of systems; a complex and dynamic network of interlocking and interdependent infrastructures (“critical national infrastructures”) whose harmonious functioning enables the myriad actions, transactions, and information flow that undergird the orderly conduct of civil society in this country. The vulnerability of these infrastructures to threats — deliberate, accidental, and acts of nature — is the focus of greatly heightened concern in the current era, a process accelerated by the events of 9/11 and recent hurricanes, including Katrina and Rita.

This report presents the results of the Commission’s assessment of the effects of a high altitude electromagnetic pulse (EMP) attack on our critical national infrastructures and provides recommendations for their mitigation. The assessment is informed by analytic and test activities executed under Commission sponsorship, which are discussed in this volume. An earlier executive report, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) — Volume 1: Executive Report* (2004), provided an overview of the subject.

The electromagnetic pulse generated by a high altitude nuclear explosion is one of a small number of threats that can hold our society at risk of catastrophic consequences. The increasingly pervasive use of electronics of all forms represents the greatest source of vulnerability to attack by EMP. Electronics are used to control, communicate, compute, store, manage, and implement nearly every aspect of United States (U.S.) civilian systems. When a nuclear explosion occurs at high altitude, the EMP signal it produces will cover the wide geographic region within the line of sight of the detonation.<sup>1</sup> This broad band, high amplitude EMP, when coupled into sensitive electronics, has the capability to produce widespread and long lasting disruption and damage to the critical infrastructures that underpin the fabric of U.S. society.

Because of the ubiquitous dependence of U.S. society on the electrical power system, its vulnerability to an EMP attack, coupled with the EMP’s particular damage mechanisms, creates the possibility of long-term, catastrophic consequences. The implicit invitation to take advantage of this vulnerability, when coupled with increasing proliferation of nuclear weapons and their delivery systems, is a serious concern. A single EMP attack may seriously degrade or shut down a large part of the electric power grid in the geographic area of EMP exposure effectively instantaneously. There is also a possibility of functional collapse of grids beyond the exposed area, as electrical effects propagate from one region to another.

The time required for full recovery of service would depend on both the disruption and damage to the electrical power infrastructure and to other national infrastructures. Larger affected areas and stronger EMP field strengths will prolong the time to recover. Some critical electrical power infrastructure components are no longer manufactured in the United States, and their acquisition ordinarily requires up to a year of lead time in routine circumstances. Damage to or loss of these components could leave significant parts of the electrical infrastructure out of service for periods measured in months to a year or more. There is a point in time at which the shortage or exhaustion of sustaining backup systems,

---

<sup>1</sup> For example, a nuclear explosion at an altitude of 100 kilometers would expose 4 million square kilometers, about 1.5 million square miles, of Earth surface beneath the burst to a range of EMP field intensities.

---



including emergency power supplies, batteries, standby fuel supplies, communications, and manpower resources that can be mobilized, coordinated, and dispatched, together lead to a continuing degradation of critical infrastructures for a prolonged period of time.

Electrical power is necessary to support other critical infrastructures, including supply and distribution of water, food, fuel, communications, transport, financial transactions, emergency services, government services, and all other infrastructures supporting the national economy and welfare. Should significant parts of the electrical power infrastructure be lost for any substantial period of time, the Commission believes that the consequences are likely to be catastrophic, and many people may ultimately die for lack of the basic elements necessary to sustain life in dense urban and suburban communities. In fact, the Commission is deeply concerned that such impacts are likely in the event of an EMP attack unless practical steps are taken to provide protection for critical elements of the electric system and for rapid restoration of electric power, particularly to essential services. The recovery plans for the individual infrastructures currently in place essentially assume, at worst, limited upsets to the other infrastructures that are important to their operation. Such plans may be of little or no value in the wake of an EMP attack because of its long-duration effects on all infrastructures that rely on electricity or electronics.

The ability to recover from this situation is an area of great concern. The use of automated control systems has allowed many companies and agencies to operate effectively with small work forces. Thus, while manual control of some systems may be possible, the number of people knowledgeable enough to support manual operations is limited. Repair of physical damage is also constrained by a small work force. Many maintenance crews are sized to perform routine and preventive maintenance of high-reliability equipment. When repair or replacement is required that exceeds routine levels, arrangements are typically in place to augment crews from outside the affected area. However, due to the simultaneous, far-reaching effects from EMP, the anticipated augmenters likely will be occupied in their own areas. Thus, repairs normally requiring weeks of effort may require a much longer time than planned.

The consequences of an EMP event should be prepared for and protected against to the extent it is reasonably possible. Cold War-style deterrence through mutual assured destruction is not likely to be an effective threat against potential protagonists that are either failing states or trans-national groups. Therefore, making preparations to manage the effects of an EMP attack, including understanding what has happened, maintaining situational awareness, having plans in place to recover, challenging and exercising those plans, and reducing vulnerabilities, is critical to reducing the consequences, and thus probability, of attack. The appropriate national-level approach should balance prevention, protection, and recovery.

The Commission requested and received information from a number of Federal agencies and National Laboratories. We received information from the North American Electric Reliability Corporation, the President's National Security Telecommunications Advisory Committee, the National Communications System (since absorbed by the Department of Homeland Security), the Federal Reserve Board, and the Department of Homeland Security. Early in this review it became apparent that only limited EMP vulnerability testing had been accomplished for modern electronic systems and components. To partially remedy this deficit, the Commission sponsored illustrative

testing of current systems and infrastructure components. The Commission's view is that the Federal Government does not today have sufficiently robust capabilities for reliably assessing and managing EMP threats.

The United States faces a long-term challenge to maintain technical competence for understanding and managing the effects of nuclear weapons, including EMP. The Department of Energy and the National Nuclear Security Administration have developed and implemented an extensive Nuclear Weapons Stockpile Stewardship Program over the last decade. However, no comparable effort was initiated to understand the effects that nuclear weapons produce on modern systems. The Commission reviewed current national capabilities to understand and to manage the effects of EMP and concluded that the Country is rapidly losing the technical competence in this area that it needs in the Government, National Laboratories, and Industrial Community.

An EMP attack on the national civilian infrastructures is a serious problem, but one that can be managed by coordinated and focused efforts between industry and government. It is the view of the Commission that managing the adverse impacts of EMP is feasible in terms of time and resources. A serious national commitment to address the threat of an EMP attack can develop a national posture that would significantly reduce the payoff for such an attack and allow the United States to recover in a timely manner if such an attack were to occur.



## Acknowledgements

The Commission is pleased to acknowledge the support of its staff, whose professionalism and technical competence have contributed substantially to this report:

- ◆ Dr. George Baker
- ◆ Dr. Yvonne Bartoli
- ◆ Mr. Fred Celec
- ◆ Dr. Edward Conrad
- ◆ Dr. Michael Frankel
- ◆ Dr. Ira Kohlberg
- ◆ Dr. Rob Mahoney
- ◆ Dr. Mitch Nikolich
- ◆ Dr. Peter Vincent Pry
- ◆ Dr. James Scouras
- ◆ Dr. James Silk
- ◆ Ms. Shelley Smith
- ◆ Dr. Edward Toton

The Commission additionally acknowledges the technical and scientific contributions of Dr. William Radasky, Dr. Jerry Lubell, Mr. Walter Scott, Mr. Paul F. Spraggs, Dr. Al Costantine, Dr. Gerry Gurtman, Dr. Vic Van Lint, Dr. John Kappenman, Dr. Phil Morrison, Mr. John Bombardt, Mr. Bron Cikotas, Mr. David Ambrose, Dr. Bill White, Dr. Yacov Haimen, Dr. Rebecca Edinger, Ms. Rachel Balsam and Mr. Chris Baker. The Commission also acknowledges the cooperation and assistance of Ms. Linda Berg; Dr. Dale Klein (former Assistant to the Secretary of Defense [Nuclear, Chemical, and Biological Matters]); the leadership of the Defense Threat Reduction Agency and its Commission liaison, Ms. Joan Pierre; Dr. Don Linger, Senior Scientist at the Defense Threat Reduction Agency; Dr. David Stoudt of the Naval Surface Warfare Center-Dahlgren; Dr. Michael Bernardin of Los Alamos National Laboratory; and Dr. Tom Thompson and Dr. Todd Hoover of the Lawrence Livermore National Laboratory.

We also acknowledge the cooperation of the Intelligence Community (IC).

The Commission was ably supported by the contracted research activities of the following organizations: the National Nuclear Security Administration's laboratories (Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Sandia National Laboratory), Argonne National Laboratory, Idaho National Laboratory, Naval Surface Warfare Center-Dahlgren, the Institute for Defense Analyses, Jaycor/Titan, Metatech Corporation, Science Applications International Corporation, Telcordia Technologies, Mission Research Corporation, and the University of Virginia Center for Risk Management of Engineering Systems.



## Chapter 1. Infrastructure Commonalities

The physical and social fabric of the United States is sustained by a system of systems; a complex and dynamic network of interlocking and interdependent infrastructures (“critical national infrastructures”) whose harmonious functioning enables the myriad actions, transactions, and information flow that undergird the orderly conduct of civil society in this country. The vulnerability of these infrastructures to threats — deliberate, accidental, and acts of nature — is the focus of heightened concern in the current era, a process accelerated by the events of 9/11 and recent hurricanes, including Katrina and Rita.

This volume focuses on a description of the potential vulnerabilities of our critical national infrastructures to electromagnetic pulse (EMP) insult, and to that end, the chapters in this document deal individually with the EMP threat to each critical infrastructure separately. However, to set the stage for understanding the potential threat under conditions in which all infrastructures are under simultaneous attack, it is important to realize that the vulnerability of the whole — of all the highly interlocked critical infrastructures — may be greater than the sum of the vulnerability of its parts. The whole is a highly complex system of systems whose exceedingly dynamic and coordinated activity is enabled by the growth of technology and where failure within one individual infrastructure may not remain isolated but, instead, induce cascading failures into other infrastructures.

It is also important to understand that not only mutual interdependence, and hence new vulnerabilities, may be enabled by technology advances, but also technologies that have facilitated this growing interdependence may be common across the many individual infrastructures. In particular, the Commission thought it important to single out the growth and common infrastructural infiltration of one particular transformative technology, the development of automated monitoring and control systems — the ubiquitous robots of the modern age known as Supervisory Control and Data Acquisition (SCADA) systems.

This opening chapter thus focuses on a more detailed description of these two aspects of modern infrastructures, control systems and mutual interdependence, that are common to all and which the Commission believes provide context and insight for understanding sources of vulnerability in all the Nation’s infrastructures to EMP attack.

### SCADA Systems

#### *Introduction*

SCADAs have emerged as critical and growing elements of a quietly unfolding industrial revolution spurred by the computer age. The accelerating penetration of SCADA systems, along with their electronic cousins, digital control systems (DCS) and programmable logic controllers (PLC), as critical elements in every aspect of every critical infrastructure in the Nation, is both inevitable and inexorable. While conferring economic benefit and enormous new operational agility, the growing dependence of our infrastructures on these omnipresent control systems represents a new vector of vulnerability in the evolving digital age of the 21st century, such as cyber security. Such issues remain as a matter for high-level concern and attention today. High-altitude EMP focuses our attention toward another potential vulnerability of these systems, and one with potentially vastly expanded consequences.



### What Is a SCADA?

SCADAs are electronic control systems that may be used for data acquisition and control over large and geographically distributed infrastructure systems. They find extensive use in critical infrastructure applications such as electrical transmission and distribution, water management, and oil and gas pipelines. SCADA technology has benefited from several decades of development. It has its genesis in the telemetry systems used by the railroad and aviation industries.

*In November 1999, San Diego County Water Authority and San Diego Gas and Electric companies experienced severe electromagnetic interference to their SCADA wireless networks. Both companies found themselves unable to actuate critical valve openings and closings under remote control of the SCADA electronic systems. This inability necessitated sending technicians to remote locations to manually open and close water and gas valves, averting, in the words of a subsequent letter of complaint by the San Diego County Water Authority to the Federal Communications Commission, a potential "catastrophic failure" of the aqueduct system. The potential consequences of a failure of this 825 million gallon per day flow rate system ranged from "spilling vents at thousands of gallons per minute to aqueduct rupture with ensuing disruption of service, severe flooding, and related damage to private and public property." The source of the SCADA failure was later determined to be radar operated on a ship 25 miles off the coast of San Diego.*

The physical form of a SCADA may differ from application to application and from one industry to another, but generally they all share certain generic commonalities. A SCADA system physically bears close resemblance to the internals of a generic desktop personal computer. Typically, it might contain familiar-appearing circuit boards, chips of various sorts, and cable connectors to the external world. The cable connectors, in turn, may be connected, perhaps quite remotely, to various sensor systems that are the SCADA's eyes and ears, as well as electronic control devices by which the SCADA may issue commands that adjust system performance. **Figure 1-1** provides an example of a particular SCADA controller that is representative of many such systems.

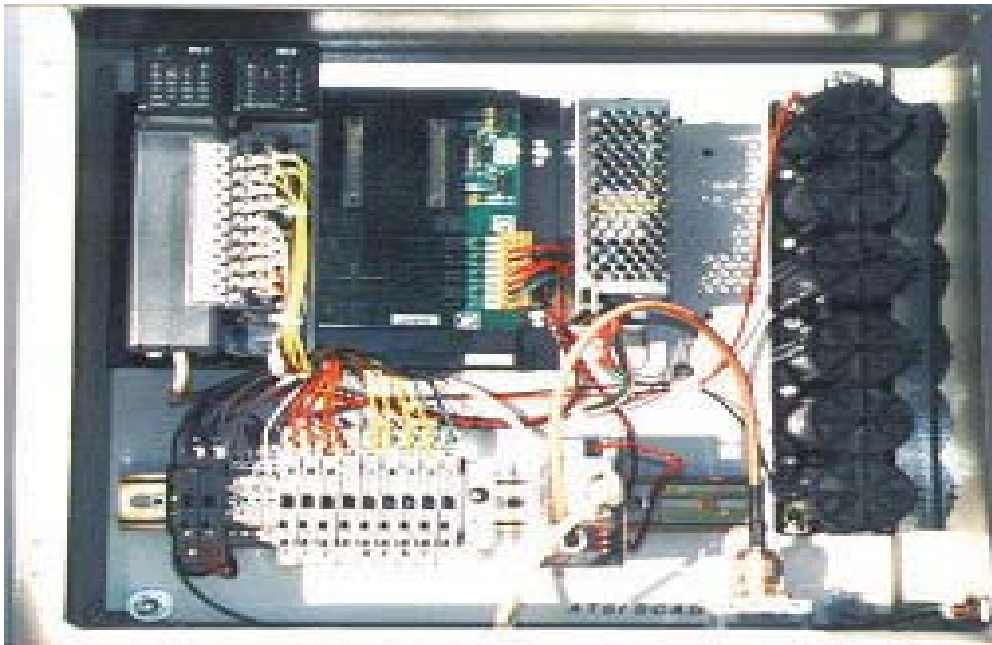


Figure 1-1. Typical SCADA Architecture

One major function of a SCADA — the data acquisition part of the acronym — is to provide a capability to automatically and remotely monitor the operating state of a physical system. It accomplishes this monitoring by providing an ongoing reporting of parameters that either characterize the system's performance, such as voltage or currents developed in an electric power plant, flow volume in a gas pipeline, and net electrical power delivered or received by a regional electrical system, or by monitoring environmental parameters such as temperature in a nuclear power plant and sending an alarm when prescribed operating conditions are exceeded.

The supervisory control function of a SCADA reflects the ability of these devices to actively control the operation of the system by adjusting its output. For example, should an electrical generating plant fail through loss of a critical hardware component or industrial accident, the monitoring SCADA will detect the loss, issue an alert to the appropriate authorities, and issue commands to other generating plants under its control to increase their power output to match the load again. All these actions take place automatically, within seconds, and without a human being involved in the immediate control loop.

A typical SCADA architecture for the electric power industry may consist of a centralized computer — the master terminal unit (MTU) — communicating through many remote terminal unit (RTU) subsystems, as illustrated in **figure 1-2**. The RTUs are used in remote, unmanned locations where data acquisition and control tasks must be performed. Examples of typical RTU data acquisition actions include processing signals from sensors such as thermocouples, voltage sensors, or power meters and reporting the state of equipment such as switch and circuit breaker positions. Typical control actions include starting and stopping motors and controlling valves and circuit breakers.

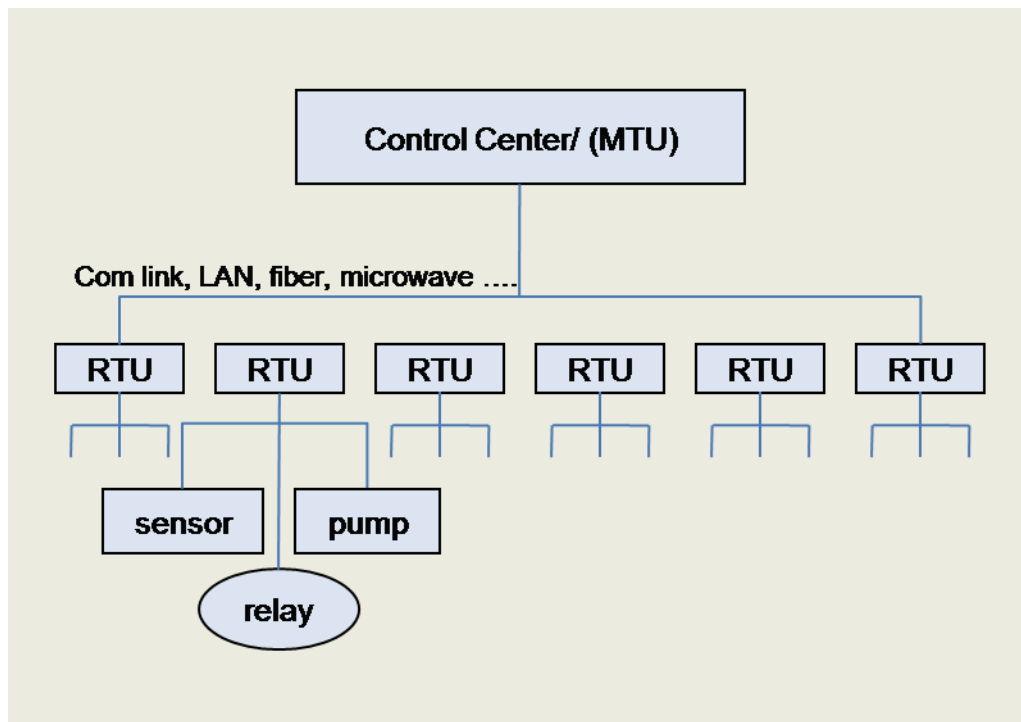


Figure 1-2. Generic SCADA Architecture

DCSs share many functional and physical hardware similarities with SCADA systems. A DCS typically will be used to control automated processes at a single location, such as

an oil refinery or a chemical plant. In contrast, a SCADA typically might be sited in an environment with dispersed assets where real-time situational awareness from remote locations is a key element of centralized control. Most DCS installations control complex, dynamic systems that would be difficult or impossible to control in a safe or economical manner using only manual control.

Even a relatively straightforward process such as electrical power generation using a conventional steam cycle requires highly complex systems to maximize efficiency, while maintaining safety and environmental protection. For example, control systems in a steam generating plant would include parameters such as generator speed, generator lubrication oil pressure, excitation current and voltage output, feed water pressure and boiler steam drum level, and air box pressure and rate of combustion.

Upset of these control points has the potential to cause severe physical damage. A case in point is the boiler endpoints of combustion and circulation. Normally, the control system would first reach the endpoint of combustion (limit of air and fuel adding energy into the boiler) and, thus, prevent any thermal damage to the boiler. If the control system is upset, it potentially could reach the endpoint of circulation (maximum rate of steam generation) or endpoint of carryover (maximum rate at which water is *not* carried out of the boiler) before the endpoint of combustion. This situation would cause thermal damage to the boiler tubes or physical damage to steam turbine blades.

Normally, a PLC is used to control actuators or monitor sensors and is another piece of hardware that shares many physical similarities to SCADAs and is often found as part of a larger SCADA or DCS system. The SCADA, DCS, and PLC systems all share electronic commonalities and, thus they share intrinsic electronic vulnerabilities as well. SCADA systems, however, tend to be more geographically disposed and exposed; our subsequent discussion focuses on SCADAs. When exposure or unprotected cable connectivity is an issue, the discussion should be considered to pertain to both PLC and DCS as well. See **figure 1-3**.

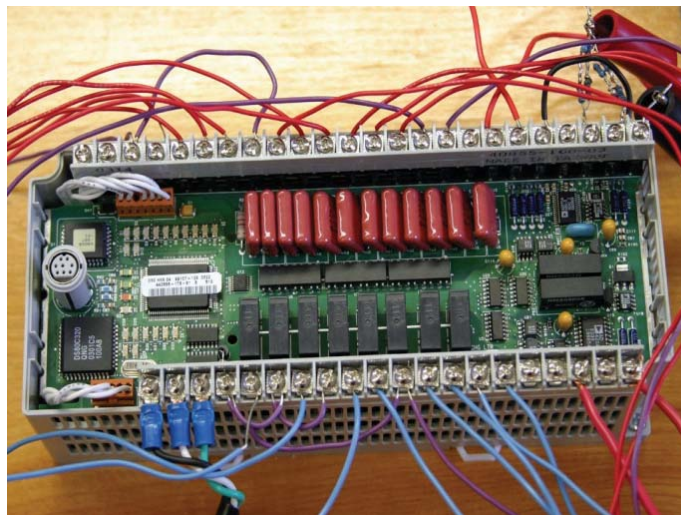


Figure 1-3. PLC Switch Actuator

### ***EMP Interaction with SCADA***

SCADA system components by their nature are frequently situated in remote environments and operate without proximate human intervention. Although their critical electronic elements usually are contained within some sort of metallic box, the enclosures'

service as a protective Faraday cage is typically minimal. Generally such metallic containers are designed only to provide protection from the elements and a modicum of physical security. They typically are not designed to protect the electronics from high-energy electromagnetic pulses that may infiltrate either from the free field or from the many antennae (cable connections) that may compromise electromagnetic integrity. The major concern for SCADA vulnerability to EMP is focused on the early time E1 component of the EMP signal. This is because, even in the power industry, SCADA systems generally are not directly coupled electrically to the very long cable runs that might be expected to couple to a late-time E3 signal.

To come to grips with the potential vulnerability of our critical national infrastructures caused by a threat to these ubiquitous SCADA control systems, we must first develop a sense of the vulnerability of the underlying hardware components themselves. To this end, the EMP Commission sponsored and funded a series of tests of common SCADA components in a government-owned EMP simulator (see **figure 1-4**). The simulation testing provided an opportunity to observe the interaction of the electromagnetic energy with equipment in an operational mode. Because the simulator did not completely replicate all characteristics of a threat-level EMP environment, observed test results can be related to the system's response in more realistic scenarios through analysis and judgment based on coupling differences between the simulated and real-world cases.



**Figure 1-4. EMP Simulator with Test Structures and Internal Electronics**

The Commission consulted with experts from industry groups associated with the North American Electric Reliability Corporation (NERC) and by site and market surveys to identify representative control systems for testing. A test matrix was developed that reflected electronic control technologies employed in power generation, power distribution, pipeline distribution, and manufacturing plants. Some test items assessed in this effort are shown in **figure 1-5**.





Figure 1-5. Some of the Electronic Control Systems Exposed in Test Facility

### ***EMP Simulation Testing***

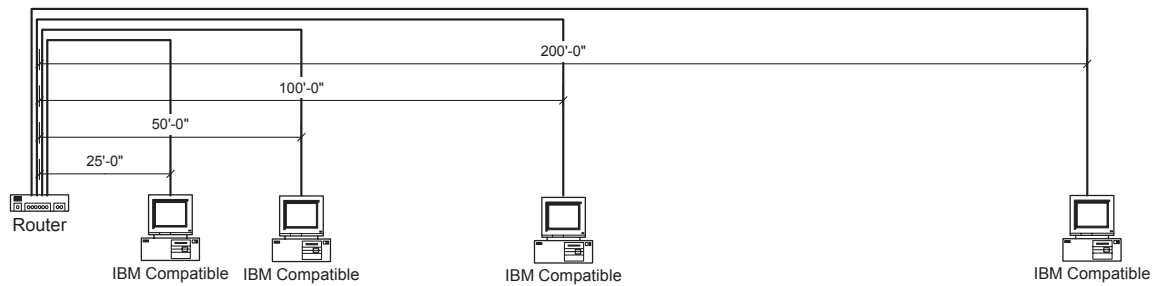
In this section, we provide a brief summary of the results of illuminating electronic control systems in the simulator. The detailed results of the simulation test program are documented separately in reports sponsored by the Commission. In Chapter 2, we provide a more complete description of the test methodology, in which we discuss testing carried out during assessment of the EMP vulnerability of the electric grid.

Many of the control systems that we considered achieved operational connectivity through Ethernet cabling. EMP coupling of electrical transients to the cables proved to be an important vulnerability during threat illumination. Because the systems would require manual repair, their full restoration could be a lengthy process. A simple model of four Ethernet cables from a router to four personal computers (PC) was generated to quantify the impact of cable length. The configuration of this model is shown in **figure 1-6**. The results of the analysis indicate that the coupling to the 200 feet of Ethernet line is roughly seven times the transient level on the 25-foot line measured during the test program. The testing and analysis indicate that the electronics could be expected to see roughly 100 to 700 ampere current transients on typical Ethernet cables. Effects noted in the EMP testing occurred at the lower end of this scale.

The bottom line observation at the end of the testing was that every system tested failed when exposed to the simulated EMP environment. The failures were not identical from system to system or within a system. For example, a device with many input-output ports might exhibit degraded performance on one port, physical damage on another, and no effect on a third. Control units might report operating parameters at variance with their post illumination reality or fail to control internal flows. The Commission considered the implications of these multiple simultaneous control system failures to be highly significant as potential contributors to a widespread system collapse.

### **Impact of SCADA Vulnerabilities on Critical Infrastructures: Historical Insight**

Based on the testing and analysis outlined in the previous section, we estimate that a significant fraction of all remote control systems within the EMP-affected area will



**Figure 1-6. Physical Model Used to Quantify Coupling to Different Cable Lengths in a Hypothetical Local Area Network (LAN)**

experience some type of impact. As the test results were briefed to industry experts at NERC and the Argonne National Laboratory, it became apparent that even minor effects noted during the testing could significantly affect the processes and equipment being controlled. Putting together a complete analysis for complex processes associated with infrastructure systems is extremely difficult. Developing the ability to analyze or model these impacts is beyond the scope of this effort.

To provide insight into the potential impact of these EMP-induced electronic system malfunctions, one can consider the details of historical events. In these cases, similar (and arguably less severe) system malfunctions have produced consequences in situations that are far too complex to predict beforehand using a model or analysis.

Another important observation is that these incidents are seldom the result of a single factor. Rather they are a combination of unexpected events that, only in hindsight, are easily related to the impact. This is not surprising given the complexity of the systems involved. Before considering the historical database, it is important to remember that historical examples, although important for the insight they provide into the dependence of a functioning modern infrastructure on its automated eyes, ears, and remote controllers, do not adequately capture the scale of the expected EMP scenario. In the latter, it is not one or a few SCADA systems that are malfunctioning (the typical historical scenario), but large numbers — hundreds or even thousands — with some fraction of those rendered permanently inoperable until replaced or physically repaired.

Significant historical events that provide insight into the potential impact of damage or upset to control systems include Hurricane Katrina; the 1996 Western States blackout; the August 14, 2003, Northeast blackout; a geomagnetic storm in 1989; the June 10, 1999, Bellingham pipeline incident; the August 19, 2000, Carlsbad pipeline incident; the July 24, 1994, Pembroke, United Kingdom, refinery incident; and a Netherlands electromagnetic interference (EMI) incident. The following paragraphs discuss the relevance of four of these incidents to an EMP event. The other four incidents — Hurricane Katrina; the Western States blackout; the August 14, 2003, blackout; and the 1989 geomagnetic storm — are described in Chapter 2, which is dedicated to a discussion of EMP effects on the electric power grid.

*Bellingham Pipeline Incident.* On June 10, 1999, one of the Olympic pipelines transporting gasoline ruptured in the Whatcom Falls Park area of Bellingham, Washington. About 250,000 gallons of gasoline from the pipeline entered the Hannah and Whatcom Creeks, where the fuel ignited, resulting in three fatalities and eight injuries. In addition, the banks of the creek were destroyed over a 1.5-mile section, and several buildings adjacent to the creek were severely damaged.



Causes included improperly set relief valves, delayed maintenance inspections, and SCADA system discrepancies. The effects all came together at the same time that changes in pipeline operations were occurring. Given the wide area of an EMP, it is conceivable that some of the pipelines affected could also suffer from poor maintenance. The electronic disturbance of an EMP event could be expected to precipitate SCADA failures and the ensuing loss of valve controls.

*Carlsbad Pipeline Incident.* On August 19, 2000, an explosion occurred on one of three adjacent large natural gas pipelines near Carlsbad, New Mexico, operated by the El Paso Natural Gas Company. The pipelines supply consumers and electric utilities in Arizona and Southern California. Twelve people, including five children, died as a result of the explosion. The explosion left an 86-foot-long crater. After the pipeline failure, the Department of Transportation's Office of Pipeline Safety (OPS) ordered the pipeline to be shut down. The explosion happened because of failures in maintenance and loss of situational awareness, conditions that would be replicated by data acquisition disruptions caused by an EMP event.

*Pembroke Refinery Incident.* On July 24, 1994, a severe thunderstorm passed over the Pembroke refinery in the United Kingdom. Lightning strikes resulted in a 0.4 second power loss and subsequent power dips throughout the refinery. Consequently, numerous pumps and overhead fin-fan coolers tripped repeatedly, resulting in the main crude column pressure safety valves lifting and major upsets in the process units in other refinery units, including those within the fluid catalytic cracking (FCC) complex.

There was an explosion in the FCC unit and a number of isolated fires continued to burn at locations within the FCC, butamer, and alkylation units. The explosion was caused by flammable hydrocarbon liquid continuously being pumped into a process vessel that, because of a valve malfunction, had its outlet closed. The control valve was actually shut when the control system indicated that it was open. The malfunctioning process control system did not allow the refinery operators to contain the situation.

As a result of this incident, an estimated 10 percent of the total refining capacity in the United Kingdom was lost until this complex was returned to service. The business loss is estimated at \$70 million, which reflects 4.5 months of downtime. The disturbances caused by the lightning strikes — power loss and degradation — would also result from an EMP event.

*Netherlands EMI Incident.* A mishap occurred at a natural gas pipeline SCADA system located about 1 mile from the port of Den Helder, Netherlands, in the late 1980s. A SCADA disturbance caused a catastrophic failure of an approximately 36-inch diameter pipeline, which resulted in a large gas explosion.

This failure was caused by EMI traced to a radar coupling into the wires of the SCADA system. Radio frequency energy caused the SCADA system to open and close at the radar scan frequency, a relay that was, in turn, controlling the position of a large gas flow-control valve. The resulting changes in valve position created pressure waves that traveled down the pipeline and eventually caused the pipeline to fail. This incident shows the potential damage to pipelines from improper control system operations, a condition that could be replicated by an EMP event.

## Summary

SCADA systems are vulnerable to EMP insult. The large numbers and widespread reliance on such systems by all of the Nation's critical infrastructures represent a systemic threat to their continued operation following an EMP event. Additionally, the necessity to reboot, repair, or replace large numbers of geographically widely dispersed systems will considerably impede the Nation's recovery from such an assault.

## Infrastructures and Their Interdependencies

### Introduction

All critical national infrastructures are fault tolerant to some degree. Design engineers and system managers are cognizant of, and fully expect, failure of subsystems and individual electrical components. Networks are designed with an expressed goal to avoid single point failures that can bring down the entire system, though in practice the evolved network may be so complicated that no one can guarantee that this design goal has been achieved. Single point failures are anticipated in the design of the systems and engineering solutions of various kinds, including redundancy, rapid repair, replacement, and operational rerouting.

It is important to note, however, that safeguards against single point failures generally depend on the proper functioning of the rest of the national infrastructure, a plausible assumption for high-reliability infrastructure systems when they experience random, uncorrelated single point failures.

Planning for multiple failures, particularly when they are closely correlated in time, is much less common. It is safe to say that no one has planned for, and few have even imagined, a scenario with the loss of hundreds or even thousands of nodes across all the critical national infrastructures, all simultaneously. That, however, is precisely the circumstance contemplated by an EMP attack scenario.

The ability to predict the consequences of failure within a critical infrastructure will require the use of reliable modeling and simulation tools. Some tools exist for the individual infrastructures and serve as either planning tools, real-time control models, or operational support elements to allocate or control resources during network outages and restoration activities.

They are generally validated within the parameter space of normal operating experience and concern, and they serve their purposes well. But it is also recognized that the systems being modeled are so complex that currently available modeling tools cannot capture the full richness of potential system responses to all possible network configurations and operating states.

Thus, for example, on the order of once a decade or so, portions of the national power grid will experience an unpredicted major disruption with failures cascading through some of the network pathways. Following the major Northeast power blackout of August 14, 2003, analysts continued to debate the cause of the disruption. The sophisticated, relatively mature, and operationally deployed modeling and simulation tools have not been able to replicate unambiguously the observed events of August 14.

◆  
“We have produced designs so complicated that we cannot possibly anticipate all the possible interactions of the inevitable failures; we add safety devices that are deceived or avoided or defeated by hidden paths in the systems.” Charles Perrow, *Normal Accidents*

The scenarios envisioned by an EMP attack involve potential failures distributed across a wide geographical extent. These include multiple combinations of node failures, a condition that generally is outside the parameter space of validation of extant system models and poses a severe challenge to predicting the subsequent evolution of the infrastructure response. The response of critical national infrastructures to an EMP attack is precisely the subject of many sections of this report. But there is a particular aspect of modeling infrastructures that is even less well developed and whose particular relevance to the EMP scenario stresses the current state of the simulation art to produce a high-fidelity simulation. That aspect is the interaction among the different infrastructures. Particularly difficult to anticipate and to capture in simulations are situations in which the occurrence of simultaneous failures can bring into play dormant and hitherto hidden interaction pathways in which a destructively synergistic amplification of failure, normally locally contained, may be propagated through the network at large.

Charles Perrow<sup>1</sup> in particular has drawn attention to these types of failures, which he has termed *normal accidents* and which are posited as an inherent property of any tightly coupled system once a threshold of complexity has been passed. The Commission believes that, given sufficient priority, time and resources, complex interdependent models can be developed to guide future assessments of the U.S. national infrastructure to EMP attack and to guide investment decisions on how best to protect our infrastructures.

### **Complex Interactions**

Various lists are in circulation that identify the critical infrastructures. The EMP Commission has chosen to address the following areas in separate sections of this Commission report:

- ◆ Electric power
- ◆ Telecommunications
- ◆ Banking and finance
- ◆ Petroleum and natural gas
- ◆ Transportation
- ◆ Food
- ◆ Water
- ◆ Emergency services
- ◆ Space
- ◆ Government

The separation of these infrastructures into different domains tends to obscure the real interdependencies that sustain the effectiveness and daily operation of each one.

As a simple example, the telecommunications infrastructure requires power that is delivered by the power infrastructure. If power delivery is disrupted by disturbances in the power grid, telecommunication substations will run for a while on reserve battery power but would then need to switch to reserve backup generators (if they have them). The generator's operation would rely on fuel, first from on-site storage and then conveyed to a central distribution point by the energy distribution infrastructure and delivered to the telecommunications substation by the transportation infrastructure and paid for by the components of the financial infrastructure. The technicians who show up,

---

<sup>1</sup> Perrow, Charles, *Normal Accidents*, Princeton University Press, Princeton, N.J., 1999.

through the transportation infrastructure, to make repairs would not do so unless they have been sustained by the food and water delivery infrastructures, and so forth. In turn, a functioning telecommunications system provides critical situational awareness and control to a power infrastructure that must keep its power generation in balance with its load in a dynamic control process over a very large geographical area. Telecommunications also plays a critical role in controlling the transportation system and is the basis of data exchange within the financial infrastructure. The complex interdependence between elements within each infrastructure is suggested and illustrated schematically but by no means wholly characterized by **figure 1-7**.

“Communicating across disciplines requires domain experts to learn one another’s language to pose significant questions and usefully interpret answers,” National Academy of Sciences, *Making the Nation Safer; The Role of Science and Technology in Countering Terrorism*

In the course of ordinary interruptions, many of these infrastructure interdependencies and interactions can be safely ignored. In an EMP attack scenario, the immediate insult is expected to affect the different infrastructures simultaneously through multiple electronic component disruptions and failures over a wide geographical area. Understanding these cross-cutting interdependencies and interactions is critical to assessing the capability of the full system of interdependent critical infrastructures to recover. The modeling and simulation needed to explore the response of such a complex situation involves a large but finite number of elements and should be amenable to analysis, at least approximately, but little effort has been made to address the problem to date.

In practice, understanding the interdependence may be a difficult task because subject area experts are not necessarily attuned to coupling mechanisms that span the boundary between their respective discipline and another, and because an accurate representation of the interdependence requires a familiarity with transdisciplinary phenomena.

Experience demonstrates that it is sometimes easy to overlook the less obvious roles that such interdependencies and interactions may play, and coupling pathways may be easily overlooked. As an example, many of the recovery procedures developed by organizations to deal with emergencies involve the implicit assumption that transportation is available and people will be put on airplanes and go somewhere to diagnose and repair something. In the immediate aftermath of 9/11, all civilian airplanes were grounded. In 1991, a single point failure inside the telecommunications system, the accidental severing of a single fiber-optic cable in the New York City region, not only blocked 60 percent of all calls into and out of New York, but also disabled all air traffic control functions from Washington, D.C., to Boston — the busiest flight corridor in the Nation — and crippled the operations of the New York Mercantile Exchange.<sup>2</sup> These key interdependencies were always there, but they were not recognized as warranting advanced contingency planning, situational awareness in degraded conditions, and operational workarounds.

<sup>2</sup> Neumann, Peter, *Computer-Related Risks*, Addison Wesley, Reading, Mass., 1995.



Infrastructure vulnerability has been the subject of recent high-level attention with three separate congressionally chartered commissions devoted to the topic, including the President's Commission on Critical Infrastructures (the Marsh Commission), the EMP Commission and The National Research Council of the National Academy of Sciences. The latter issued a report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* in 2002, which explores potential vulnerabilities in the same list of critical infrastructures cited in the previous section. Both commissions noted the lack of a mature modeling and simulation capability as a significant weakness in the protective toolset available to planners and those charged with the mission of shielding our key infrastructures from subversion or other disruption. The National Academy of Sciences study, in particular, recommended the development of an analytic capability based on systems engineering principles.

Critical infrastructure studies also have been a growing activity in academia with the participation of individual scholars at various universities around the country. A number of academic centers have also set up or spun off entire institutes devoted to the analysis of critical infrastructural matters. The University of Virginia has created the Center for Risk Management, which focuses on the application of input-output econometric models



to analysis of critical infrastructures. In addition, George Mason and James Madison universities in Virginia have created the Center for Infrastructure Protection Programs (CIPP). The Santa Fe Institute of Complexity Studies also has pursued important theoretical work, and there are many other examples as well.

These efforts, as well as other important related work, are pointing in the right direction. Nevertheless, the bottom-line is that currently an adequate capability to model individual infrastructures on a national scale does not exist. Moreover, the capability to develop and integrate a fully interactive and coupled set of national-scale infrastructure models is not being pursued with sufficient priority and support to achieve it in the foreseeable future.

### **Commission-Sponsored Modeling and Simulation (M&S) Activities**

As the Commission embarked on its task, it attempted to engage existing capabilities within academia, industry, and government to simulate the behavior of infrastructures subjected to stressful disruption. To that end, it initiated the following activities.

*National Workshop.* The EMP Commission sponsored a national workshop on the modeling and simulation of interdependent interacting infrastructures as part of an effort to understand the state of modeling capability in this country and to identify capabilities that might be exploited to provide insight into the expected effects of a prescribed EMP attack scenario. A number of national experts who are working on related modeling and simulation activities participated. The Commission has exploited some of these capabilities to develop insight that helped inform the assessment provided by the Commission's full report.

*Contractual Activities.* Current modeling and simulation tools are not sufficient to provide a realistic predictive capability for the interdependent infrastructures. Nevertheless, the modeling capability proved useful in developing the Commission's insight into the effects of coupling on the overall impact due to the attack and the expected recovery and restoration effort. The Commission examined such questions as: Does a strong or weak coupling tend to drive the models to longer or shorter infrastructure restoration times? What seemed to be the sensitive parameters? What sorts of decoupling activities might be suggested to shorten reconstitution efforts? The examination of these and similar questions was supported by a number of efforts the Commission initiated with the NISAC, the University of Virginia, and Argonne National Laboratory. Some of the results of these efforts are summarized in the following section.

*EMP Commission Staff Analyses.* The EMP Commission staff also developed analytic products to explore issues of stability and instability related to infrastructural coupling models. In particular, the Commission focused on models that coupled the power to the telecommunication infrastructure in an interactive way.

The results of these efforts have informed the Commission's findings, as documented in this volume.

### ***Illustrative Modeling and Simulation Results for Coupled Infrastructures***

To illustrate some of the complex behavior that can arise when coupling between infrastructures is included, consider the simple case of the interaction of only two infrastructures, here taken to be the telecommunication and power networks. The telecommunication networks themselves are in the midst of a rapid evolution that has seen data communications, which represented only 10 percent of the total traffic in 1990, grow to about 50 percent of the daily telecommunications load, with the expectation that voice traffic will

---



represent only a small fraction of the traffic by 2015. There is a corresponding ongoing evolution, both in the network architecture and the underlying hardware, that is described in more detail in Chapter 3 of this report.

A critical element of the network of the future will be reliance on public data networks (PDNs). In the past, the electric power grid relied on its own communication system to monitor and control the grid, and mutual dependence between the power and telecommunications systems was essentially nil. Today the power grid relies on PDNs for about 15 percent of its telecommunication needs, and this figure is expected to grow to 50 percent in the near future. **Figure 1-8** illustrates the expected interdependence for this evolving network.

The PDNs represent networks powered by the power distribution network. The power generation and distribution network is, in turn, controlled by SCADA systems that depend on telecommunications to provide situational awareness and to execute control functions for the power grid. **Figure 1-9** represents the results of a model simulation. The telecommunication network reverts back to a dependence on commercial power while both are in the recovery phase. The power infrastructure continues to depend in part on the probability of call blocking, while the recovery for telecommunications depends on the available power.

The figure shows four distinct phases of a recovery process — an early phase extending to about a half hour, during which many network elements execute reinitializations to restore some service with power generally available from battery backup, to a phase of interdependency, during which the only power option left is reliance on the commercial grid, which in turn is dependent on a commercial PDN. This model can provide insight into the recovery process. It predicts significantly lengthened recovery times because of infrastructure interdependency, compared to recovery analysis that examines an infrastructure in isolation, ignoring the factor of interdependency. While illustrative of the effects of interdependency, this model is not meant to represent the actual behavior of any specific real-world system today.

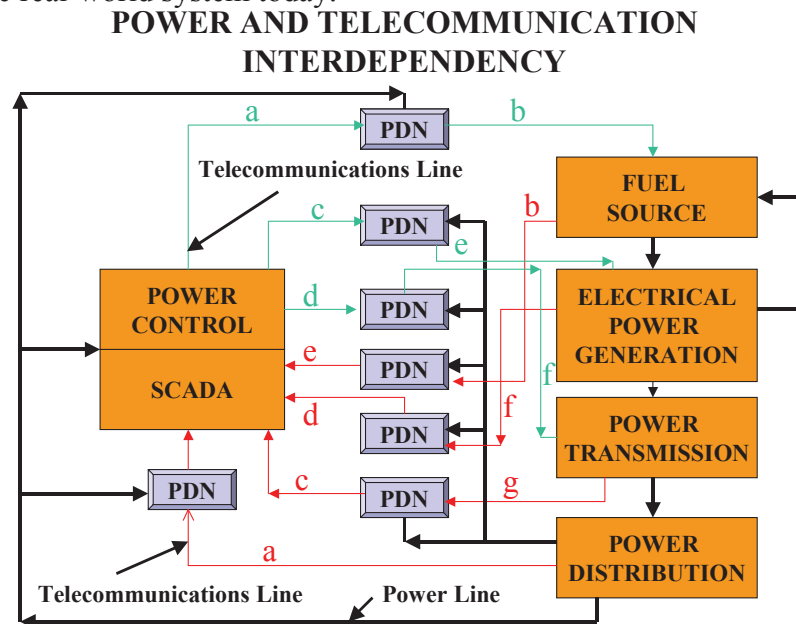
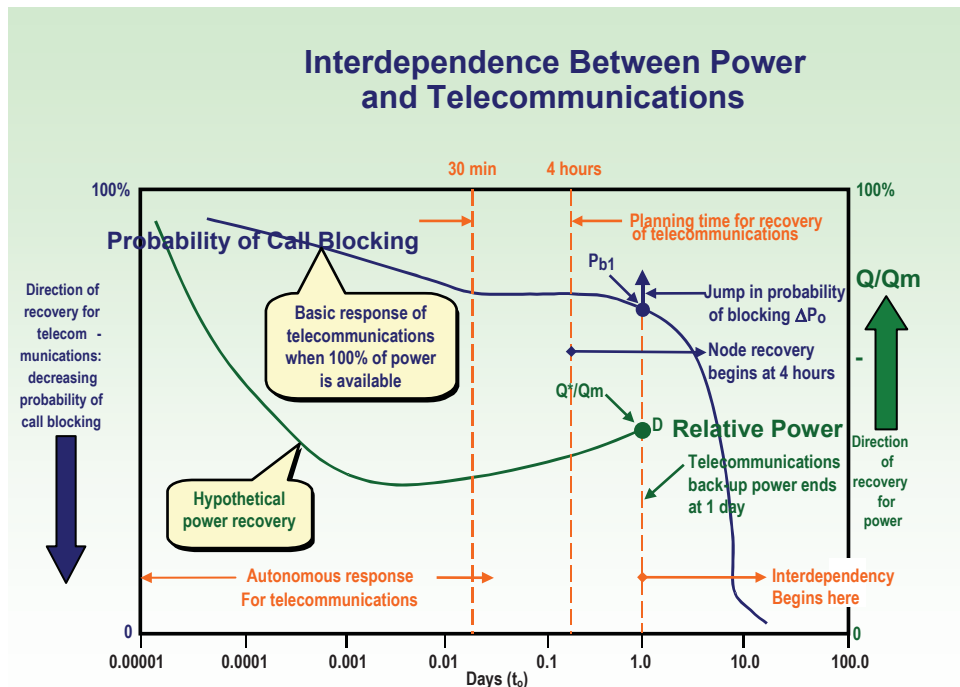


Figure 1-8. Interdependency for Anticipated Network of the Future

Figure 1-9. Results of a Model Simulation<sup>3</sup>

In another effort, the NISAC studied the consequences of an EMP attack scenario<sup>4</sup> involving a large EMP source located at high altitude off the California coastline. The simulation looked at the effects on water, electric power, telecommunications, natural gas, refined petroleum products, transportation, labor and economic sector productivity and attempted to capture their known interactions. The simulation included network models for the transfer of information and infrastructure products, services, markets, and process models for each product and service. The boundary conditions for the simulation were provided by the EMP Commission; for study purposes, they included descriptions of the potential initial states of both the power and telecommunication infrastructures immediately following exposure to the EMP environment. The simulation, which was not considered realistic because it did not consider likely physical damage that would impede any recovery process, was still useful in providing insight into the potential for disturbances in one infrastructure to cascade into others.

## Summary

No currently available modeling and simulation tools exist that can adequately address the consequences of disruptions and failures occurring simultaneously in different critical infrastructures that are dynamically interdependent. Many infrastructure models that do exist are local to regional in scope.

The Federal Government is supporting a number of initiatives to develop critical national infrastructure modeling and simulation capability as a national analysis and planning resource. However, these are not high national priorities and are funded at less

<sup>3</sup> Kohlberg, Clark, and Morrison, "Theoretical Considerations regarding the Interdependence between Power and Telecommunications," preprint, EMP Commission Staff Paper.

<sup>4</sup> Brown and Beyeler, "Infrastructure Interdependency Analysis of EMP Effects and Potential Economic Losses," EMP Commission Interdependencies Modeling and Simulation Workshop, Washington, D.C., June 2003.

than critical mass. They also are fragmented and uncoordinated, which is not an entirely negative observation, as the complexity of the task merits exploration of independent research and development approaches.

Recent analytic work suggests that evolving interdependencies may be inadvertently introducing entirely new and potentially serious vulnerabilities that could lead to infrastructure failures, even without the precipitating catalyst of an EMP attack.

### **Recommendations**

- ◆ The Commission recommends that research be conducted to better understand infrastructure system interdependencies and interactions, along with the effects of various EMP attack scenarios. In particular, the Commission recommends that such research include a strong component of interdependency modeling. Funding could be directed through a number of avenues, including through the National Science Foundation and the Department of Homeland Security.
- ◆ The Commission recognizes current interest in protecting SCADA systems from electronic cyber assault. The Commission recommends that such activities be expanded to address the vulnerability of SCADA systems to other forms of electronic assault, such as EMP.

## Chapter 2. Electric Power

### Introduction

The functioning of society and the economy is critically dependent upon the availability of electricity. Essentially every aspect of American society requires electrical power to function. Contemporary U.S. society is not structured, nor does it have the means, to provide for the needs of nearly 300 million Americans without electricity. Continued electrical supply is necessary for sustaining water supplies, production and distribution of food, fuel, communications, and everything else that is a part of our economy. Continuous, reliable electrical supply within very tight frequency boundaries is a critical element to the continued existence and growth of the United States and most developed countries.

For most Americans, production of goods and services and most of life's activities stop during a power outage. Not only is it impossible to perform many everyday domestic and workplace tasks, but also people must divert their time to dealing with the consequences of having no electricity. In the extreme, they must focus on survival itself. The situation is not different for the economy at large. No other infrastructure could, by its own collapse alone, create such an outcome. All other infrastructures rely on electric power. Conversely, the electric power infrastructure is dependent on other infrastructures that are themselves vulnerable to the direct effects of electromagnetic pulse (EMP) in ways that are described elsewhere in this report. No infrastructure other than electric power has the potential for nearly complete collapse in the event of a sufficiently robust EMP attack. While a less robust attack could result in less catastrophic outcomes, those outcomes would still have serious consequences and threaten national security.

The electrical power system is the largest single capital-intensive infrastructure in North America. It is an enormously complex system of systems containing fuel production, gathering and delivery systems, electrical generators (often themselves systems), electrical transmission systems, control systems of all types, and distribution systems right down to the electrical outlet and interconnection at the point of use. It is this vast array of systems and components all acting in concert, integrated into a cohesive whole to deliver electrical power at the point of use, with supply-on-demand at a uniform frequency that provides the reliable, steady, and adequate electric supply on which everyone has come to expect and depend. Because of the integration and interdependence of the electric system's components and the ever growing shift to electronics and particularly microelectronics for operation, protection and control, the Nation is particularly vulnerable to a major disruption of the electric supply.

Today, the existing electrical system at peak demand periods increasingly operates at or near reliability limits of its physical capacity. Modern electronics, communications, protection, control and computers have allowed the physical system to be utilized fully with ever smaller margins for error. Therefore, a relatively modest upset to the system can cause functional collapse. As the system grows in complexity and interdependence, restoration from collapse or loss of significant portions of the system becomes exceedingly difficult. Over the last decade or two, relatively few new large-capacity electric transmission capabilities have been constructed and most of the additions to generation capacity that have been made have been located considerable distances from load for environmental, political, and economic reasons, adding stress and further limiting the system's ability to withstand disruption. Significant elements of the system, including many generating plants, are aging (a considerable number are more than 50 years old)

and becoming less reliable or are under pressure to be retired for environmental considerations, further exacerbating the situation.

Should the electrical power system be lost for any substantial period of time, the Commission believes that the consequences are likely to be catastrophic to civilian society. Machines will stop; transportation and communication will be severely restricted; heating, cooling, and lighting will cease; food and water supplies will be interrupted; and many people may die. “Substantial period” is not quantifiable but generally outages that last for a week or more and affect a very large geographic region without sufficient support from outside the outage area would qualify. EMP represents such a threat; it is one event that may couple ultimately unmanageable currents and voltages into an electrical system routinely operated with little margin and cause the collapse of large portions of the electrical system. In fact, the Commission is deeply concerned that such impacts are certain in an EMP event unless practical steps are taken to provide protection for critical elements of the electric system and to provide for rapid restoration of service, particularly to essential loads.

The electrical power system routinely experiences disruptions. In most cases, the cause is the failure of one or a small number of components. The overall system has a degree of durability against such failures, although in some cases failures lead to a cascading loss of power up to a regional level that extends over relatively short to moderate periods of time. The current strategy for recovering from such failures is based on the assumption of sporadic failures of small numbers of components, and for larger failures, drawing on resources from outside the affected area. This strategy leaves us ill-prepared to respond effectively to an EMP attack that would potentially result in damage to vast numbers of components nearly simultaneously over an unprecedented geographic scale.

The Commission recognizes that EMP is one of several threats to the overall electrical power system. Some of these threats are naturally occurring, such as geomagnetic storms. Others, like attacks using information operations on the system’s controls, are manmade. There are strong similarities in the types of damage resulting from the occurrence of such threats. There are also similarities in the measures that are appropriate to be undertaken to reduce the electrical power system’s vulnerability to each of these threats. The Commission believes that the measures it recommends will both reduce the vulnerability of the electrical power system to these threats and improve the Nation’s ability to recover the system.

The magnitude of an EMP event varies with the type, design and yield of the weapon, as well as its placement. The Commission has concluded that even a relatively modest-to-small yield weapon of particular characteristics, using design and fabrication information already disseminated through licit and illicit means, can produce a potentially devastating E1 field strength over very large geographical regions. This followed by E2 impacts, and in some cases serious E3 impacts operating on electrical components left relatively unprotected by E1, can be extremely damaging. (E3 requires a greater yield to produce major effects.) Indeed, the Commission determined that such weapon devices not only could be readily built and delivered, but also the specifics of these devices have been illicitly trafficked for the past quarter-century. The field strengths of such weapons may be much higher than those used by the Commission for testing threshold failure levels of electrical system components and subsystems.

Additionally, analyses available from foreign sources suggest that amplitudes and frequency content of EMP fields from bomb blasts calculated by U.S. analysts may be too low. While this matter is a highly technical issue that awaits further investigation by U.S. scientific experts, it raises the specter of increased uncertainty about the adequacy of current U.S. EMP mitigation approaches.

A key issue for the Commission in assessing the impact of such a disruption to the Nation's electrical system was not only the unprecedented widespread nature of the outage (e.g., the cascading effects from even one or two relatively small weapons exploded in optimum location in space at present would almost certainly shut down an entire interconnected electrical power system, perhaps affecting as much as 70 percent or possibly more of the United States, all in an instant) but more significantly widespread damage may well adversely impact the time to recover and thus have a potentially catastrophic impact.

For highly dependent systems such as commercial telecommunications and the financial system, electric power is frequently filtered through batteries. These act to condition the power as well as to provide limited backup. Local, at-site emergency generators are used quite extensively for high priority loads. These include hospitals, cold storage, water systems, airport controls, rail controls and similar uses. These systems, however, are themselves increasingly dependent on electronics to initiate start up, segregate them from the larger power system, and control their operating efficiency, thereby rendering them vulnerable to EMP.

Furthermore, emergency generators have relatively short-term fuel supplies, generally less than 72 hours. Increasingly, locally stored fuel in buildings and cities is being reduced for fire safety (after 9/11) and environmental pollution reasons, so that emergency generation availability without refueling is becoming even more limited. Batteries normally have a useful life well short of emergency generators, often measured in a few hours. All of these tools for maintaining a stable and adequate power supply, even to high priority loads, are intended to be temporary at best – bridging the time until restoration can take place.

The impact of such an EMP-triggered outage would be severe but not catastrophic if the recovery was rapid or the geographic impact sufficiently limited. The recovery times from previous large-scale outages have been on the order of one to several days. This record of quick recovery is attributable to the remarkably effective operation of protective systems and communications that are an essential part of the power infrastructure and the multiple sources of replacement components from surrounding nonimpacted systems. In this context, a short blackout scenario over a relatively small geographic region would be economically painful. Of the more than \$10 trillion U.S. Gross Domestic Product, about three percent is electricity sales. However, estimates of economic loss from historical blackouts range from factors of six (for domestic customers) to 20 (for industrial users) times the value of the interrupted service. By these measures, the economic impact of an outage is between 18 and 60 percent of total production in the affected area. Again, this estimate is for reasonably short-lived blackouts. A short blackout presents no threat to national survival.

On the other hand, a geographically widespread blackout that involves physical damage to thousands of components may produce a persistent outage that would far exceed historical experience, with potentially catastrophic effect. Simulation work sponsored by the

---



Commission at the National Infrastructure Simulation and Analysis Center (NISAC) has suggested that, after a few days, what little production that does take place would be offset by accumulating loss of perishables, collapse of businesses, loss of the financial systems and dislocation of the work force. The consequences of lack of food, heat (or air conditioning), water, waste disposal, medical, police, fire fighting support, and effective civil authority would threaten society itself.

The Commission solicited technical assistance and judgment from the North American Electric Reliability Corporation (NERC, which is governed by the Federal Energy Regulatory Commission [FERC] guidelines); utilities with particularly relevant experience (such as with geomagnetic storms [similar to E3]; long or very high voltage transmission; uniquely sensitive generation, special fault testing; and similar aspects); suppliers of protection, control, and other related equipment; groups dealing with industry standards; organizations of utilities, fuel suppliers, fuel transportation groups; select academic, national, and internationally recognized experts, the Department of Energy (DOE) National Laboratories, and relevant governmental entities. Willingness to be helpful was uniformly positive and generous. The Commission is grateful for this support.

NERC was uniquely well suited to be of assistance. NERC was established in the aftermath of the 1965 Northeast Power Failure to enhance the reliability of the electrical system. The Commission briefed the NERC Board of Trustees on the nature of the threat and the potential vulnerability. The NERC Board established an EMP task force under the aegis of its Critical Infrastructure Protection Advisory Group to provide technical advice to the Commission. The expertise of the task force membership spanned the three NERC Interconnects (Eastern, Western States Coordinating Council [WSSC], and Electric Reliability Council of Texas [ERCOT]), and all three major categories of the system (generation, transmission, and distribution).

This group's involvement was an essential element in focusing the Commission on the importance of the early-time EMP pulse and its implications for recovery, as well as on other triggers of widespread impact. It also provided technical input that was very helpful in implementing and interpreting a Commission-sponsored test program targeted at identifying the threshold at which significant control and protective components for the electrical system would begin to fail through disruption, false data, and damage. Many of the technical and operational insights discussed within the report were influenced by this task force although the NERC Task Force did not otherwise directly participate in the drafting of the report or in its conclusions.

## Description

### **Major Elements**

There are three major elements of the electrical power infrastructure: (1) generation, (2) transmission (relatively high voltage for long distances), and (3) distribution, whose elements are interdependent, yet distinct (see **figure 2-1**).

**Generation.** Power plants convert energy that is in some other form into electricity. The initial form of the energy can be mechanical (hydro, wind, or wave), chemical (hydrogen, coal, petroleum, refuse, natural gas, petroleum coke, or other solid combustible fuel), thermal (geothermal or solar), or nuclear. Power plants can range from single solar cells to huge central station complexes. In most circumstances the first stage of generation

converts the original form of energy into rotational mechanical energy, as occurs in a turbine. The turbine then drives a generator.

## Power System Overview

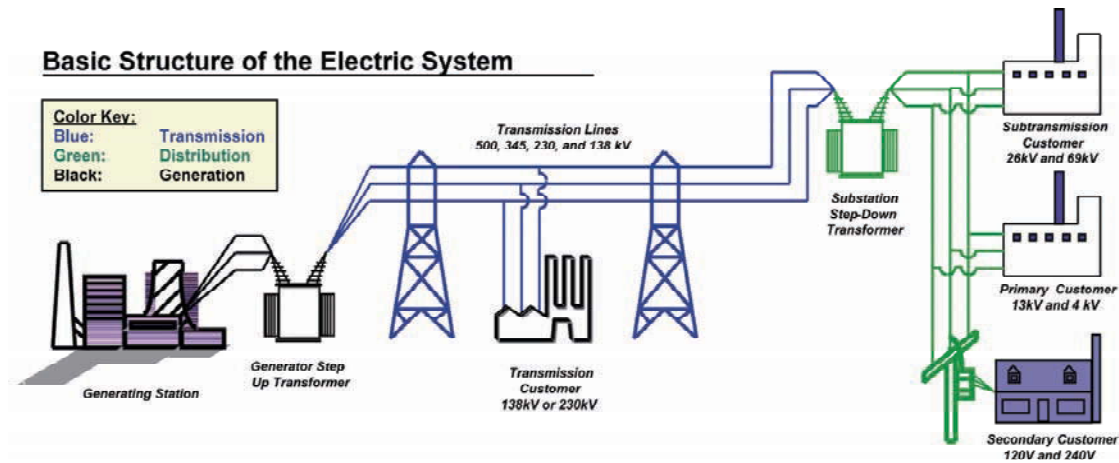


Figure 2-1. Power System Overview

Modern power plants all utilize complex protection and control systems to maximize efficiency and provide safety. They all have common electrical characteristics in order for them to be useable by all the various purposes to which electricity is put. Electronics have largely replaced all the electromechanical devices in older plants and are used exclusively in plants of the past one or two decades. Even generator exciters now have microprocessors and analog-to-digital converters. These electronics and, thus, the power plant itself are highly vulnerable to EMP assault. Identifying and locating damaged generation plant equipment with electronic sensors and communication interdicted and/or unreliable due to EMP and repairing the system would be a complex and time-consuming process, even when personnel and parts are readily available.

The fossil fuel supply system (coal, oil, wood, and natural gas) is largely dependent on electronics for its production and delivery of adequate fuel to the generators to produce nearly 75 percent of the Nation's electricity. There should not be a direct and immediate impact on the fuel supply for a nuclear power plant. The interdependency between the fuel necessary to generate electricity and the electricity and electronics to deliver the fuel is critical to the recovery. For example, natural gas normally is delivered just in time while oil and coal have some at-site storage. Nuclear generation supplies a major portion of the remainder of the Nation's electricity. It is unlikely for the timing of an EMP attack to be such that it would directly and immediately impact the fuel supply for a nuclear power plant. Of the balance, hydroelectric plants have their own fuel supplies as do geothermal, solar, and wind systems. However, wind and solar may or may not be generating in any event, given their inherent uncertainty. Hydro and geothermal are significant capabilities, but they are highly localized.

**Transmission.** Electrical power from the various power plants travels over a system of lines and substations to the regions and locales where it will be consumed. The transmission system moves large amounts of power generally over substantial distances and/or to directly serve very large electrical loads. This definition separates it from the distribution system, which is described below. Transmission includes lines (wires strung from insu-

lator strings on towers or underground in special insulated containers) and substations (nodal points where several lines intersect and protection and control functions are implemented). Within substations there are transformers (which transform power from one voltage to another); breakers (similar to on-and-off switches able to handle the large amounts of energy passing through); and protective devices, meters, and data transmitting and control systems. Protective devices protect the electrical components from unusual electrical disturbances that occur from time to time for many different reasons as well as for general safety reasons.

The delivery of electrical power across or through some medium, such as a wire, encounters resistance, which itself takes power to overcome. Electrical power is measured by the product of voltage and current. The electrical resistive losses (restricting the flow) are proportional to the square of the current. Thus it is most efficient to transmit power at the minimum current that is practical (this results in the highest voltage for the same amount of power). Otherwise, more power is consumed just to push the electricity through or over a path with higher resistance.

Standard values for modern alternating current (AC) transmission line voltage range from 115 kV (115 thousand volts) to 765 kV, although some 1100 kV transmission has been developed and tested. The current carried by these lines is typically up to a few thousand amperes. Direct current (DC) is also used in some instances for moving large amounts of power great distances and for controlling the flow itself. The normal point of use of electricity is AC and thus the shift from AC to DC and back from DC to AC makes DC uneconomical other than in special circumstances. The use of DC is increasing, however, as power costs continue to grow and the technology to shift from AC to DC and back becomes less expensive. Transformers within the substations are used to move the voltage from one line or power plant up to or down to another voltage while maintaining essentially the same level of power.

*Distribution.* Loads or end users of electricity (residences, commercial establishments, and even most industry) require electrical power to be available in the voltages needed in adequate supply when they need it. This often means in relatively small quantities at low voltage and current. The size of the wires and switches in a typical house are able to be quite small and of much lower cost because the power available to that house is restricted to be relatively low. The electrical and electronic appliances similarly need only a small amount of power to be available. Therefore, the high-voltage power of the transmission system described previously is reduced (stepped down) through transformers and distributed to the end users in levels they need and can use. Reactive load balancing equipment is also part of the distribution system. This equipment is needed for system stability. The electrical power system's stability is finely tuned and fragile. Large-scale failures most often occur because the system is destabilized by local anomalies.

The distinction between transmission and distribution is sometimes a fuzzy one because it depends on the size and need of the load and the specific system involved. The distinction is relevant for regulatory and business purposes. It does vary somewhat from region to region. Traditionally distribution distances are under 20 miles and voltages are less than 69.5 kV (more commonly 13.5 kV). However voltages up to 115 kV are used in some locations. Distribution has substations just like transmission, only smaller. These are not manned. Of importance is that the local switching, controls, and critical equipment have become largely electronic with concomitant vulnerability to EMP.

Alternating current, as opposed to direct current, is the medium for use of electricity as a general matter. Electricity production, transmission, distribution, and use require a precise frequency. Thus it is necessary across the vast electrical power system to precisely and reliably synchronize the frequency and phase of power coming from different generating sources and reaching and being utilized by different loads. Testimony to the accuracy of this control has been the wide use and dependence on electric clocks and the functioning of many electronic devices. The difficulty of maintaining the frequency synchronization during off-normal conditions is usually a factor in large-scale power outages. For example, when the frequency moves very far from a constant required level, protective schemes at the generators within the transmission system and at the loads alarm and often automatically trip. Occasionally these trip out of proper sequence causing the system to compound rather than mitigate the problem, and the system collapses.

*Control and Protection Systems.* Overlaid on these three primary elements — generation, transmission and distribution — is a control system that directs the power where it is needed, maintains the frequency, and protects the system. Control is also necessary for commercial aspects. The controls must protect the system from transients such as lightning, correct synchronization errors by activating reactive sources or loads, isolate malfunctioning elements of the grid, and prevent self-damage from improper compensation or human error. The control systems also enable the deregulated energy marketplace by tracking the origin, route, and destination of the energy commodity. Central to the monitoring and coordination of the power grid is a broad class of devices called supervisory control and data acquisition (SCADA) systems. These conform to an agreed set of standards that make it possible to network many such systems over a generic communications system, regardless of modality. SCADA devices are in broad use in a variety of applications other than power.

The revolution in communication, information, system and component protection, and control technologies has reached essentially every segment of the economy, and its heavy impact on the electric power industry is no exception. The growing dependence of our infrastructures on ubiquitous electronic control and protection systems confers great benefits in terms of economic and operational efficiency, rapid diagnosis of problems, and real-time remote control. At the same time and less often remarked, it also represents a potential new vector of vulnerability that could be exploited by determined adversaries, and intellectual efforts to mitigate such threats have been engaged. The infrastructure's vulnerability to EMP and other broad-impact events raises the threat to an entirely new and vastly expanded plane of serious to catastrophic impacts.

Electronics have enabled electric power systems — generation, transmission, and distribution — to achieve greater levels of efficiency and safety with much lower adverse environmental impacts. Far less generation, transmission, and distribution are now necessary to provide the same amount of benefit to the end user, thus significantly enhancing productivity and overall quality of life. In doing so, however, the electrical system operates closer to theoretical capacity and thus at narrower margins of safety and reliability. Electronics have improved system economics and lowered the overall cost of power to the end user while reducing pressure on basic resources and limiting potential adverse impacts on the environment. This enhanced capability, both on the provider and consumer side, is in part responsible (along with the regulatory environment) for the low rate of investment in the high-value components of the electric system infrastructure. For

example, slowly increasing electrical transmission demand has largely been met within the limits of current production capacity for these components.

The continuing evolution of electronic devices into systems that once were exclusively electromechanical, enabling computer control instead of direct human intervention and use of broad networks like the Internet, results in ever greater reliance on microelectronics and thus the present and sharply growing vulnerability of the power system to EMP attack. Just as the computer networks have opened the possibility to cyber assault on the power system or to electrical power system collapse associated with software failure (as during the August 14, 2003, blackout), they have provided an opportunistic pathway for EMP attack that is likely to be far more widespread, devastating, and difficult to assess and restore. Switches, relays, and even generator exciters now have microprocessors and analog-to-digital converters. These and other low-power electronics cannot be expected to withstand EMP-generated stresses unless they are well protected. Protection must encompass both device design and system integration. Even a well-designed system installed without regard for EMP intrusion via connecting lines can be rendered inoperative by EMP stress. There is a serious question regarding whether manual control of the system sufficient to allow continued service will be possible even at a much-reduced state in the aftermath of EMP.

The key vulnerable electronic systems are SCADA along with digital control systems (DCS) and programmable logic controllers (PLC). SCADAs are used for data acquisition and control over large and geographically distributed infrastructure systems while DCSs and PLCs are used in localized applications. These systems all share similar electronic components, generally representative of components that form the internal physical architectures of portable computers. The different acronyms by which we presently identify SCADA, DCS, and PLC should not obscure the fact that the electronics have evolved to the point where the differing taxonomies are more representative of the functional differences of the electronics equipment rather than differences in the electronics hardware itself.

Electronic control equipment and innovative use of electronic controllers in equipment that is not usually considered control equipment are rapidly replacing the purely electromechanical systems and devices that were their predecessors. The use of such control equipment is growing worldwide, and existing users are upgrading equipment as new functionalities develop. The U.S. power industry alone is investing about \$1.4 billion annually in new SCADA equipment. This is perhaps 50 times the reinvestment rate in transformers for transmission. The present rate represents upgrade and replacement of the protection and control systems to ever more sophisticated microelectronics at roughly 25 to 30 percent annually, with each new component more susceptible to EMP than its predecessor. The shift to greater electronic controls, computers, and the Internet also results in fewer operators and different operator training. Thus the ability to operate the system in the absence of such electronics and computer-driven actions is fast disappearing. This is almost certain to have a highly deleterious effect on restoring service in the event of an EMP attack.

### ***Electrical System Organization***

The integrated electrical power system of the United States and integrated systems in Canada and Mexico are covered by the NERC. This vast network is broken into only three truly separate systems at the present time — the Eastern Interconnection, the

---



Western Interconnection, and Texas. The dividing line geographically between the Eastern and Western systems is roughly a line between Montana and North Dakota continuing southward. The largest of these, the Eastern Interconnection, serves roughly 70 percent of the electrical load and population of the United States. The three regions are separated electrically in AC in order to provide barriers for transfer of major frequency deviations associated with system separations. This mode of operation between regions is referred to as maintaining frequency independence. Importantly, this also acts as a barrier to EMP-caused system disruption or any other major system disruption and consequent collapse crossing between these three regions.

In **figure 2-2** the map of the three NERC regions shows the divisions geographically and the barriers for transfer of major frequency deviations associated with system separations. There are some nonsynchronous connections, such as DC back-to-back converter installations that facilitate limited power transfers yet maintain a barrier. The subregions identified in the map within a region are for organizational, record keeping, and management only. They do not have frequency independence from one another at this time. Thus at present, whole regions can be caused to collapse by sufficiently large electrical disturbances, like EMP, which severely exacerbates the problem of service to critical loads and importantly impedes restoration where delay increases the adverse impacts virtually exponentially.

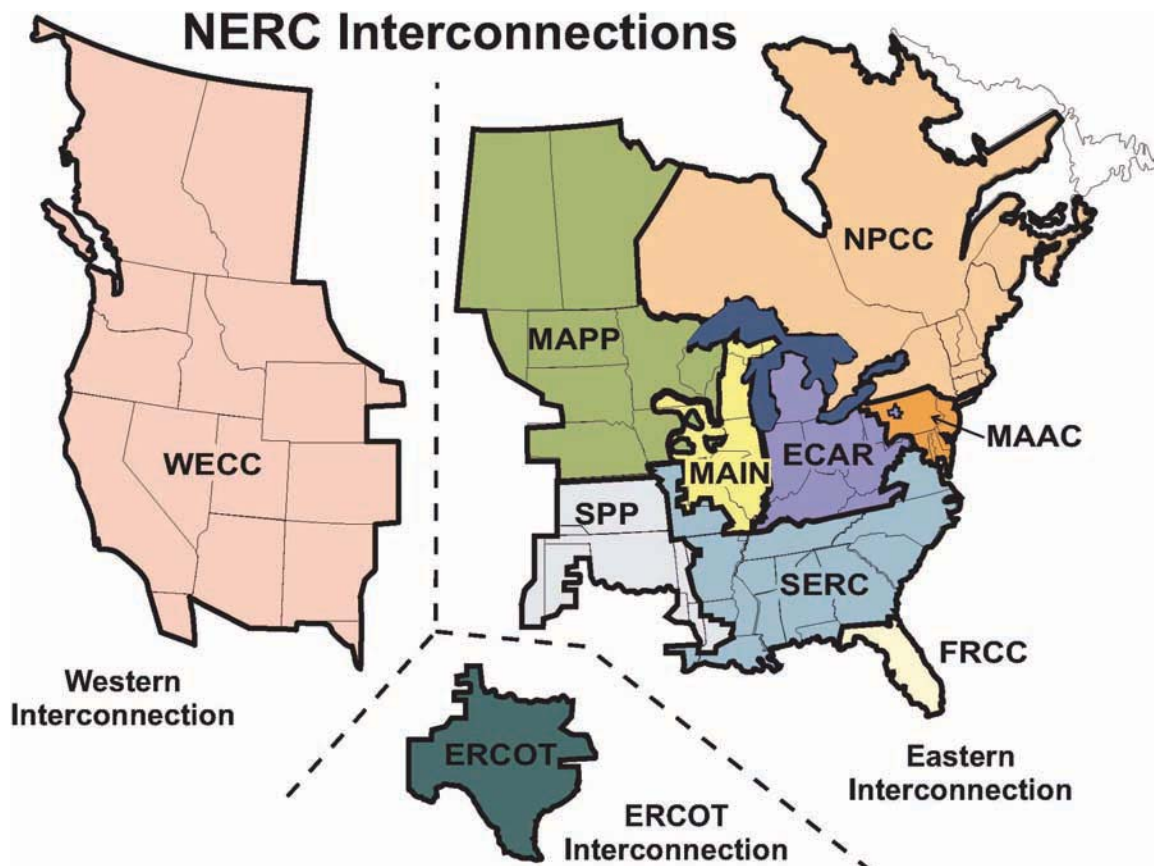


Figure 2-2. NERC Interconnections

### Capacity Reserves

Although greater conservation and efficiency at the end user has reduced the need for new generation largely through the use of improved electronics and controls, the growing



economy and use of ever greater labor- and material-saving devices continues to drive the need for new generation. Furthermore, older generation is being replaced for economic, environmental, and locational reasons. Increasing capital costs emanating from world market competition and natural disasters, plus the increasing cost of capital, have slowed the addition of new generation capacity. The inability in many cases to get generation to market with reasonable assurance due to limited transmission has similarly limited new generation additions. Finally, regulatory returns and pressure from competing uses of capital within utility systems or their parents, including municipal and public systems, have further restricted new generation of consequence. As a result, generation capacity margins have decreased.

Changes in the regulatory environment with greater deregulation of the generating sector have further encouraged recent increases in new generation capacity along with retirement of older units. Most of the new power plants over the past decade or two have been natural gas-fired units that are agile in their ability to adapt to market demands and opportunities, are relatively clean environmentally for fossil plants, faster to build and have lower capital cost than many alternative generator options. They have been located farther from load in most instances than the older plants or previously planned additions, and they are operated and integrated very differently than in the past as economic decisions are often driven by very diverse and nonintegrated responsibility. This can stretch the ability of the transmission system to get the new generation to load. The type and location of new generation stresses the system and increases its vulnerability to various threats including EMP.

The capacity margin (standby capacity for emergencies or other unplanned needs) for the transmission system grid (system of higher voltage lines and substations) has decreased from about 20 percent twenty years ago to about 10 percent now as an overall system matter although there are considerable regional or local variations. This reduced margin is due to little new construction, improved efficiency of the existing system, and the location of new generation away from load. It is further exacerbated by the addition of significant generation from renewable resources such as wind energy, which operates when the wind blows, not when the electrical system might otherwise require power. This results in shifting the generation between the wind and other controllable generation on an unpredictable basis regardless of the transmission system reliability needs, all of which results in greater and less predictable stresses on the overall system.

Operation of the transmission system at today's reduced margin while maintaining excellent reliability has been enabled by improved technology and operating practices for protection, command, and control of the transmission grid. While power production and consumption have grown, almost all of the growth has been absorbed on existing power lines although new substations have been added. There has been very little construction of transmission capacity, particularly of new longer distance transmission lines, or renewal and replacement of existing infrastructure for many reasons, including deregulation (discussed in the next section of this chapter). The transmission system thus is operating with little ability to absorb adverse electrical impacts.

Overall, as a result of reduced generation capacity margins, the generation component of the system is far less able to compensate for the difficulties that may be encountered within the transmission system and vice versa. Together, the consequence is a power system far more vulnerable to disruption than in the past, and this vulnerability is increasing.

While greater protection and control schemes have still provided a very reliable system in spite of this, the system is being stressed beyond reasonable limits. The electrical power system has become virtually fully dependent upon electronic systems working nearly flawlessly. The overall system reliability is testimony to the skill and effectiveness of the control systems. However, the lack of margin (combination of generation and transmission margins) results in making catastrophic cascading outages far more likely, and should the electronics be disrupted, the system is highly likely to fail on a broad scale. Thus, the small margin and reliance on electronics give rise to EMP vulnerability.

High-value assets (assets that are critical to the production and delivery of large volumes of electrical power and those critical for service to key loads) in the system are vulnerable to EMP through the loss of protection equipment due to E1 and even if E3 levels were not large enough to cause damage. The largest and most critical of these are transformers. Transformers are the critical link (1) between generation and transmission, (2) within the transmission network, (3) between the transmission and distribution systems, and (4) from the distribution to the load.

The transformers that handle electrical power within the transmission system and its interfaces with the generation and distribution systems are large, expensive, and to a considerable extent, custom built. The transmission system is far less standardized than the power plants are, which themselves are somewhat unique from one to another. All production for these large transformers used in the United States is currently offshore. Delivery time for these items under benign circumstances is typically one to two years. There are about 2,000 such transformers rated at or above 345 kV in the United States with about 1 percent per year being replaced due to failure or by the addition of new ones. Worldwide production capacity is less than 100 units per year and serves a world market, one that is growing at a rapid rate in such countries as China and India. Delivery of a new large transformer ordered today is nearly 3 years, including both manufacturing and transportation. An event damaging several of these transformers at once means it may extend the delivery times to well beyond current time frames as production is taxed. The resulting impact on timing for restoration can be devastating. Lack of high voltage equipment manufacturing capacity represents a glaring weakness in our survival and recovery to the extent these transformers are vulnerable. Distribution capability is roughly in the same condition although current delivery times are much less (i.e., limited manufacturing capability, although there is domestic production).

### ***Deregulation***

At least a decade ago, the power systems were owned and operated by vertically integrated utility companies. These entities consisted of investor-owned (owned by shareholders, commonly referred to as private) utilities, utilities that are government constructs (federal, such as the Tennessee Valley Authority, Bonneville Power Administration, and others), consumer-owned cooperatives, municipalities, and entities of the state such as peoples and public utility districts. The different entities were granted monopoly powers for service and were regulated through a variety of mechanisms including self-regulation for some of the government entities. In any given service territory, the local utility owned the generation, transmission, and distribution and was responsible for adequate supply, reliability, and other aspects of service quality.

This situation has changed. On April 24, 1996, FERC issued Orders 888 and 889, which encouraged wholesale power supply competition, deregulating this single aspect of

the electrical industry. This allowed any party to produce and sell power to any other party at the wholesale levels (meaning sales to utility or load-serving entities, as opposed to direct retail sales to end users). Existing generation by investor-owned utilities was forced to be divested in many circumstances. This regulation applied only to the investor-owned utilities comprising a bit more than half the total U.S. electrical load. Many governmental or public entities did not possess generation of their own, and some that did followed by example and market imperatives. In some instances states have carried the deregulation further to a variety of forms of competition at the retail level.

The transmission infrastructure has remained regulated, and the previous vertically integrated systems in many instances were not allowed to commercially control their transmission in order to free up competition at the wholesale levels. Due to the complexity of an open market using an infrastructure that was built for another operating environment, the requirements for investment in the transmission system have been uncertain and more expensive. FERC regulates the transmission facilities in terms of use and pricing, but not location. The federal transmission regulation paradigm is moving toward being market based, which will have unknown impacts but is believed to assist in the development of new transmission facilities. The states also play an important role in the regulation of transmission and generation that is not consistent from state to state. With the market (and the market model itself) in flux, there is unwillingness presently to invest in transmission infrastructure.

There is no incentive for the states or localities to accede to construction of lines that are to move power over or through the state or locality without direct benefit to such state or locality. The power going through the lines pays no fees and no taxes to the hosts, although there are minor property taxes on the physical facilities in some instances. Until recently there was no capability to track the path of a given unit of energy when operating in AC and even then it is more calculation via model-specific than actual measurement. This is because AC power travels over the path of least resistance not as the flow of power might be contracted. Thus while a new interconnected line may appear to carry power pursuant to a contract for delivery between two parties, it is unlikely that the power will flow physically as envisioned. Thus it is unclear who will pay for the use of the new line. While new capability to track AC power (E-tags) could provide the basis for fiscal incentives for new line construction, it is not yet widely deployed nor well understood or accepted. Moreover, regulatory requirements create impediments to new line construction even if the incentives and capital are at hand. In short, from a business perspective, transmission lines are often low return or loss centers in the current environment.

The end state of the regulatory paradigm is still undetermined, and this uncertainty coupled with lack of local benefits when passing through state and local areas all contribute to the diminishing transmission capacity margins. There is uncertainty whether, by the time construction of new lines is completed, the investment could be recovered. It is likely that this situation will persist until the market model is clarified and implemented, which may take several years given the complexity and number of competing interests, including between the states and the Federal Government as well as with neighboring states. The market and system reliability pressure may move this faster as recognition and evidence mount. As noted earlier, the reduced and diminishing margins contribute significantly to EMP vulnerability.

## Vulnerabilities

In order to assess the nature of EMP effects on the electrical system, we separately analyzed the potential effects of an electromagnetic pulse on each of the three main constituents of the power system — generation, transmission, and distribution. Within the context of a principal finding of the NERC EMP task force, recovery following an EMP-caused outage within any reasonably acceptable time is contingent largely on preventing damage to the high-value assets (assets that are critical to the production and delivery of large volumes of electrical power and those critical for service to key loads) and identifying and replacing ones that become damaged. Therefore, the Commission focused on identifying what those high value assets might be and their susceptibility to EMP damage. Thus, proper design, installation, and functioning of the protective equipment for these assets during an EMP attack are critical. There are other critical aspects to recovery that are discussed subsequently.

### Generation

A power plant is designed to protect itself in the event of instantaneous loss of load, electrical faults or trips on the interconnected transmission system or internally, frequency excursions beyond rather tight limits, and often for the loss of an external power source for proper shutdown. None of these conditions should damage a power plant if the protective systems function properly, as frequently has been demonstrated. Very little damage to generation has occurred in previous blackouts, including the August 14, 2003, blackout. However, some malfunctioning in the multiple controls throughout a power plant does occur, albeit rarely. Therefore, on a broad enough scale, as in an EMP attack affecting many power plants at once, damage to a small number of these power plants would be expected statistically. Since E2 and E3 are not assessed as direct threats to the generation system (except for their step-up transformers and associated breakers), the critical vulnerability question is E1-induced plant control system failure.

The E1 pulse can upset the protection and control system, including damaging control and protective system components, and cause the plant to trip or trigger emergency controlled shut down. Current, temperature, pressure, frequency, and other physical parameters are monitored by the control systems. These provide independent measurements of same system, and all can cause the plant to trip off line and go to controlled shut down. Given the redundancy of protective system design, either several protective devices or devices in the critical path would have to fail in order for the plant not to initiate protective shutdown. However, if the control system itself or secondary nodal controls and receivers critical to orderly shut down are themselves damaged, as is reasonably possible with E1, then the plant is seriously at risk. Power plants, particularly newer ones, are highly sophisticated, very high-speed machines, and improper shut down can damage or destroy any of the many critical components and can even cause a catastrophic failure. Nuclear plants are an exception due to the nature of their protection schemes.

Given the range of potential E1 levels, analysis and test results provide a basis to expect sufficient upset to cause a plant's system to shut down improperly in many cases. Proper shutdown depends on synchronized operation of multiple controllers and switches. For example: coal intake and exhaust turbines must operate together or else explosion or implosion of the furnace may occur. Cooling systems must respond properly to temperature changes during shut down or thermal gradients can cause boiler deformation or rupture. Orderly spin-down of the turbine is required to avoid shaft sagging and blades impacting the casings. Bearings can easily fail and freeze or damage the shaft if the shut

---

down does not engage emergency lubrication. There are similar issues inside very complex machines operating at high temperatures at fast speeds with tight tolerances. Thus, power plant survivability depends on a great many protective systems creating multiple pathways to plant damage and failure.

Restoration of some damage can be very long term, certainly months and in some instances years. The loss of generation of any size itself would contribute to systemwide collapse and certainly would limit restoration. Manufacturers of generation plant protection and control equipment performed some limited evaluation and while there are layers of redundancy, as noted, more and more these systems are going to computer-controlled microelectronics, and thus are more susceptible to EMP disruption.

At the device level, power plant protective systems are less exposed than the corresponding systems in the transmission grid. They act on local information, so failure of telecommunications systems is not as much of an issue for plant protection where operators are available in most instances 24/7 and can independently assess the situation and act. The control equipment, protective systems, sensors, and current transformers typically (but by no means always) will be inside the plant although this does not necessarily mean they will not be exposed. In general there will be no outside cable runs, so the building itself will provide some EMP protection. However the lengths of these interior cables can be on the order of 100 meters. Cable trays may or may not provide additional protection, depending on their material and installation method. The key is not device- or component-level testing for EMP susceptibility but overall control and protective system test to evaluate vulnerability. Subjecting an entire sophisticated and modern power plant to testing is not feasible. However, it does not take many damaged plants out of the many hundreds to seriously impact the system operation and the ability to restore service. The fact that all power plants exposed to E1 EMP will be illuminated simultaneously (within one power cycle) makes the situation extremely serious.

#### *System Restoration — Generation*

The restoration of the system from collapse is very complex in operation, almost an art rather than a science, and it requires highly trained and experienced operators with considerable information and controls at hand. Basically, in isolated cases or when beginning restoration, a load and generation source has to be identified and interconnected without interference from other loads or generation. These are then matched and gradually restored together. Thereafter, each increment of generation and load is added in turn to a larger operating system of generation and load. As each component of load and generation are included, the frequency will be impacted. If it varies outside very tight limits, it will all trip off and have to be put back together again. In most system disruptions leading to blackouts, there are large amounts of system still intact on the periphery of the disruption, which are able to greatly assist in the restoration, more easily allowing and absorbing each addition of generation and load until all is restored.

Every generator requires a load to match its electrical output as every load requires electricity. In the case of the generator, it needs load so it does not overspin and fail, yet not so much load it cannot function. In a large integrated system, where increments of load and generation are not sufficient to cause the frequency to drop or rise above acceptable margins, it is relatively straightforward and commonplace, just as turning on a lightswitch causes a generator someplace to pick up the load. In the case where the sys-



tem is being restored and there are few loads and generators connected, this matching requires careful management and communication between load and generation.

Generation start-up for most plants requires power from another source to drive pumps, fans, safety systems, fuel delivery, and so on. Some, like hydroelectric and smaller diesels can start directly or from battery sources assuming they can control their access to matching load. In the case of EMP, large geographic areas of the electrical system will be down, and there may be no existing system operating on the periphery for the generation and loads to be incrementally added with ease. Furthermore, recovery of lost generation would be impacted by the loss of other infrastructure in varying degrees according to the type of plant. In that instance, it is necessary to have a “black start”: a start without external power source. Coal plants, nuclear plants, large gas- and oil-fired plants, geothermal plants, and some others all require power from another source to restart. In general, nuclear plants are not allowed to restart until and unless there are independent sources of power from the interconnected transmission grid to provide for independent shutdown power. This is a regulatory requirement for protection rather than a physical impediment. What might be the case in an emergency situation is for the Government to decide at the time.

Black-start generation is that kind of generator that is independent of outside power sources to get started, hence the term black start. Most black start units today are hydroelectric plants, small gas peaking units, small oil-fired peaking units and diesel units. In some cases the black start unit may be collocated with a larger power plant in order to get the larger one started for system restoration. Fuel supply would then be the only issue from the generation perspective; for example, a gas plant might not have the fuel due to EMP damage someplace in the delivery system. Assuming the black start units were not damaged by EMP or have been repaired and assuming they are large enough to be significant, workers can begin the system restoration as building blocks from the generation side of the equation. EI may have also damaged their startup electronics, which will need to be repaired first. It is often the case that generation capable of black start is not manned, so if they fail to start remotely, a person will need to be dispatched to find the problem, locate the needed parts, and get it operating. There are not many black start-capable units in locations that are suitable to independent restoration at this time. Recovery in most regions therefore needs to wait for other areas to restore power and then be reconnected increment by increment.

Even if partially disabled control systems successfully protect the critical generating equipment, all affected plants would face a long process of testing and repairing control, protective, and sensor systems. Protective and safety systems have to be carefully checked out before start up or greater loss might occur. Repair of furnaces, boilers, turbines, blades, bearings, and other heavy high-value and long lead-time equipment would be limited by production and transportation availability once at-site spares are exhausted. While some spare components are at each site and sometimes in spare parts pools domestically, these would not cover very large high-value items in most cases, so external sources would be needed. Often supply from an external source can take many weeks or several months in the best of times, if only one plant is seeking repair, and sometimes a year or more. With multiple plants affected at the same time, let alone considering infrastructure impediments, restoration time would certainly become protracted.



### ***Transmission***

Most generation is located outside major population areas and thus sometimes at great distances from the load being served. In general, electricity often travels great distances on an efficient high-voltage transmission system. The transmission system is made up of different owners, voltage levels, and controls. Yet power must be routed to where it is needed, so there are nodes called substations where the power lines join and are switched, and where power is moved from one voltage level to another level, interconnected with other transmission system components, and sent on to distribution systems. Finally as it gets closer to load, power is stepped down (reduced in voltage) and then down again and often down yet again to and within the distribution system and then normally down again to the delivery point for the load. Each of those step-down points requires a transformer to effect the change and breakers to isolate the transformer when necessary.

In the event of the loss of a generation facility, a fully functional transmission system can move the remaining generation from whatever plants can operate to areas otherwise affected by loss of a particular generating station. This occurs in normal practice as generation plants are brought in and out of service for one reason or another. The same thing happens when part of the transmission system is down for whatever reason. Other transmission in the network picks up the loss and generation is shifted so that the loads can continue to be served. All this is accomplished regularly as part of system operation. The ability to adjust quickly given access to a multitude of resources, generation, and transmission makes the system reliable. Incapacitation of sufficient elements of the transmission system would mean the inability to deliver power whether the generation is available or not. The same inability would be true for incapacitation of sufficient generation. In the case of EMP, both would be likely to be impacted simultaneously. This is what results in a blackout where the load does not get served. The transmission system is highly vulnerable to EMP.

Substation control systems at the nodes or hubs in the transmission system are inherently more exposed to the E1 pulse than their power plant counterparts, which are often not in buildings at all. The sensors, communications, and power connections are outdoors and cables (i.e., antennas in the sense of an EMP receptor) which may be hundreds of meters long may be buried, run along the ground, or elevated. The control devices themselves, including the protective relays, may even be in remote structures that provide little electromagnetic attenuation. Most substations do not have operators present but are remotely controlled from power dispatch centers, in some instances hundreds of miles away.

Operation of transmission substations depends on various communications modalities, including telephone, microwave, power line communications, cell phones, satellite phones, the Internet, and others. Typically, these modes are used for dedicated purposes; they do not necessarily provide a multiple redundant system but are “stove piped.” From the point of view of managing routine system perturbations and preventing their propagation, NERC advises us that the telephone remains the most important mode. If the voice communications were completely interrupted, it would be difficult, but still reasonably possible, to successfully continue operations — provided there were no significant system disruptions. However in the case of an EMP event with multiple simultaneous disruptions, continued operation is not possible. Restoration without some form of communication is also not possible. Communication is clearly critical in the path to restoration.

Just as in the case involving power plants, the first critical issue is the proper functioning of the protective elements, specifically relays, followed by the local control systems. These elements protect the high-voltage breakers and transformers that are high-value assets. High-value assets are those that are critical to system functioning and take a very long time to replace or repair. Other protected devices, such as capacitors and reactive power generators, are also high value and nearly as critical as the transformers. E1 is likely to disrupt and perhaps damage protective relays, not uniformly but in statistically very significant numbers. Left unprotected, as would likely result from E1 damage or degradation to the protective relays, the high-value assets would likely suffer damage by the transient currents produced during the system collapse, as well as potentially from E2 and E3 depending upon relative magnitudes. Commission testing of some typical protective relays with lower than expected EMP levels provides cause for serious concern.

The high-value transmission equipment is subject to potentially large stress from the E3 pulse. The E3 pulse is not a freely propagating wave like E1 and E2, but the result of distortions in the Earth's magnetic field caused by the upper atmosphere nuclear explosion. The distortion couples very efficiently to long transmission lines and induces quasi-direct current electrical currents to flow. The currents in these long lines can aggregate to become very large (minute-long ground-induced currents [GIC] of hundreds to thousands of amperes) sufficient to damage major electrical power system components. With respect to transformers, probably the hardest to replace quickly, this quasi-direct current, carried by all three phases on the primary windings of the transformer, drives the transformer to saturation, creating harmonics and reactive power. The harmonics cause transformer case heating and over-currents in capacitors potentially resulting in fires. The reactive power flow would add to the stresses on the grid if it were not already in a state of collapse. Historically, we know that geomagnetic storms, which can induce GIC flows similar to but less intense than those likely to be produced by E3, have caused transformer and capacitor damage even on properly protected equipment (see **figure 2-3**). Damage would be highly likely on equipment unprotected or partially protected due to E1.



**Figure 2-3. GIC Damage to Transformer During 1989 Geomagnetic Storm**

The likelihood and scope of the E3 problem are exacerbated by the small transmission margins currently available. The closer a transformer is operating to its performance limit, the smaller the GIC needed to cause failure. Moreover, newer transmission substations are increasingly using three single-phase transformers to handle higher power transfer, since the equivalently rated three-phase transformers are too large to ship. The three-phase systems are more resistant to GIC, since their design presumes a balanced three-phase operation. Thus the separate single-phase transformers are more susceptible to damage from GIC.

#### *System Restoration — Transmission*

The transmission system is the lynch pin between generation and load. It is also a network interconnecting numerous individual loads and generating sources. To restore the overall power system to get generation to load, as noted earlier, an increment of genera-

tion needs to be matched to an increment of load and then add the next matching increments and so on. As the number of increments becomes greater, there is some flex in the system to absorb variations. As a result, the restoration is easier and goes much faster. In the initial increments however, the transmission system link between generation and load has to be isolated so other loads, which may well remain connected, do not impact the effort. This is tricky and requires careful coordination to adjust the breakers in the substations so the link is routed correctly and safely.

The power transmission grid is designed to break into islands of hopefully matched generation and load when the system receives a sufficient electrical disruption. This is both to protect service in the nonimpacted regions and to allow for the stable systems to be used to restart the island that lost functionality. With EMP, broad geographic reach and simultaneous multiple levels of disruption result in a situation in which the islanding schemes themselves will probably fail to work in the EMP-affected area. Since the geographic area is so large, perhaps encompassing an entire NERC region or possibly more, restoring the system from the still functioning perimeter may well not be possible at all or would take a great deal of time; the Commission estimates weeks to months, at least in the best circumstance.

### ***Distribution***

Most of the long power outages that Americans have experienced were due to physical damage to the distribution system — local damage. This damage is usually caused by natural events such as weather. Windblown trees fall on neighborhood power lines or ice buildup drops lines that in some instances make contact with live lines causing arcs that in turn can even result in distribution transformers exploding.

EMP damage to the distribution system would be less dramatic than that inflicted upon the transmission system but still would result in loss of load. The principal effect of EMP would be E1-induced arcing across the insulators that separate the power lines from the supporting wood or metal poles. The arcing can damage the insulator itself and in some cases result in pole-mounted transformer explosions. Damage to large numbers of insulators and pole-mounted transformers could also result in a shortage of replacement parts, as these items are fairly reliable under normal conditions, and spares are not kept to cover widespread losses. Ultimately workarounds and replacements can be found in most circumstances although widespread damage and impact to related infrastructures will cause delay.

The important effect of the loss of load in the EMP scenario is that it happens simultaneously. Thus it represents a substantial upset to the entire grid, causing the frequency to spin up and protective relays to open on generation and can by itself result in a cascading failure and blackout of the entire NERC region. Similarly, any consumer or industrial electrical device that is shut down or damaged by EMP contributes to the load loss and further drives the system to collapse. It becomes a case of what comes first to cause what failure since the EMP E1 impulse is virtually simultaneously disrupting all facets of the electrical system and load.

### ***Synergistic Effects of E1, E2, and E3***

The effects of EMP on the electrical power system are fundamentally partitioned into its early, middle, and late time effects (caused by the E1, E2, and E3 components, respectively). The net impact on the electric power grid includes the synergistic interaction of all three, occurring nearly simultaneously over a large geographic area. The

---

Commission has concluded that the electrical system within the NERC region so disrupted will collapse with near certainty. Thus one or more of the three integrated, frequency-independent NERC regions will be without electrical service. This loss is very large geographically and restoration is very likely to be beyond short-term emergency backup generators and batteries. Any reasonable EMP event would be much larger than the Texas region so basically the concern is the Eastern and Western regions with Texas either included or not depending upon the location of the weapon. The basic threat to U.S. society that moves an EMP event from a local or short-term adverse impact to a more prolonged and injurious event is the time it takes to restore electrical and other infrastructure service.

The early time EMP, or E1, is a freely propagating field with a rise time in the range of less than one to a few nanoseconds. E1 damages or disrupts electronics such as the SCADA, DCS, and PLC as well as communications and to some extent transportation (necessary for supplies and personnel). This disrupts control systems, sensors, communication systems, protective systems, generator systems, fuel systems, environmental mitigation systems and their related computers, as well as the ability to repair. SCADA components, in particular, are frequently situated in remote environments and operate without proximate human intervention. While their critical electronic elements are usually contained within some sort of metallic box, the enclosures' service as a protective Faraday cage is inadequate. Such metallic containers are designed only to provide protection from the weather and a modicum of physical security. They are not designed to protect the electronics from high-energy electromagnetic pulses, which may infiltrate either from the free field or from the many antennae (cable connections) that compromise electromagnetic integrity.

The E1 pulse also causes flashovers in the lower voltage distribution system, resulting in immediate broad geographic scale loss of electrical load and requiring line or insulator replacement for restoration.

The intermediate time EMP, or E2, is similar in frequency regime to lightning, but vastly more widespread, like thousands to millions of simultaneous lightning strikes, even if each strike is at lower amplitude than most naturally occurring lightning. The electrical power system has existing protective measures for lightning, which are probably adequate. However, the impact of this many simultaneous lightning-like strike disruptions over an extremely large geographic area may exceed those protections. The most significant risk, however, is synergistic because the E2 pulse follows on the heels of the E1. Thus where E1-induced damage has circumvented lightning protection, the E2 impact could pass directly into major system components and damage them.

The late time EMP, or E3, follows E1 and E2 and may last for a minute or more. The E3 pulse is similar in a great many respects to geomagnetic effects induced by solar storms. Solar storms and their impacts on electrical systems with long lines have been thoroughly evaluated and are known to cause serious damage to major electrical system components at much lower levels than the reasonably possible E3 impact. This damage has been incurred in spite of functioning, in-place protective systems. Given the preceding E1 and E2 pulse damage to the protective systems and other system components, damage from E3 to unprotected major system components is virtually assured.

EMP is inimical to the continued functioning of the electrical power system and the reliable behavior of electronics. Each of the three EMP modes of system insult is suffi-



cient by itself to cause disruption and probable functional collapse of large portions of the interconnected electrical power system at EMP threat levels. In every EMP attack, all three assaults (E1, E2, and E3) are delivered in sequence and nearly simultaneously. It is the Commission's assessment that functional collapse of the electrical power system region within the primary area of assault is virtually certain. Furthermore, widespread functional collapse may result even from a small weapon with a significant E1 component. While stopping electrical supply over a broad geographical area nearly instantaneously is damaging, it is the time it takes to restore service that is important, assuming restoration is possible, which itself may be questioned in some instances.

### **System Collapse Scenarios**

NERC was one of several key advisers on the EMP impact assessment discussed above although the conclusions and emphasis are the Commission's alone. NERC also informed the Commission that there is no modeling capability extant, either deterministic or statistical, that can assess with confidence the outcome of simultaneous, combined subsystem failures. Putting together a coherent picture of the projected system collapse scenario must rely on expert judgment.

Large-scale load losses in excess of 10 percent are likely at EMP threat levels. Instantaneous unanticipated loss of load, by itself, can cause system collapse. This is possible at 1 percent loss, and is very likely above 10 percent. At similar percentage levels, loss of generation can also cause system collapse. Both the load loss (normally from a transmission system failure) and generation loss resulting in system collapse have been experienced. At the levels of loss for each, collapse is highly likely if not certain. Systemwide ground-induced currents in the transmission grid can by themselves cause system collapse. They did so in March 1989 in Quebec. At the levels expected in an E3 event, collapse would be much more likely and widespread.

Loss of computer control of substation switchyard equipment could, by itself, lead to system collapse. Manual operation is possible only with adequate communication and the ability of personnel to physically get to the right substations, a problematic question in the event of an EMP attack. Adequate numbers of trained and experienced personnel will be a serious problem even if they could all be contacted and could make themselves available. Thus manual operation would be necessary and might not be timely enough or have sufficient skilled personnel to deal with a broad-scale, instantaneous disruption and dynamic situation. Loss of manual control of switchyard equipment would, in short order, lead to line and transformer faults and trips. Several substations tripping nearly simultaneously would lead itself to system collapse.

Loss of telecommunications would not, by itself, cause immediate system collapse except as needed to address issues caused by the above disruptions. However the lack of telemetered control data would make the system operators effectively blind to what is going on, but personnel at substations, if they can get there and communicate with the system operators, could overcome much of that. Malfunction of protective relays could cause system collapse by contributing to several of the above scenarios through misinformation or by operating incorrectly.

All of these collapse mechanisms acting simultaneously provide the unambiguous conclusion that electrical power system collapse for the NERC region largely impacted by the EMP weapon is inevitable in the event of attack using even a relatively low-yield device of particular characteristics.

---

### ***Damage Scenarios***

The level of damage depends primarily on the functioning of the protective equipment, but it also depends on various aspects of the collapse. In an EMP event, the collapse is virtually instantaneous. The size of the transients on the system may be greater than existing protective systems are capable of handling, even those not damaged by the EMP itself.

Damage to the large transformers and other high-value equipment is directly related to protective relay failure, although it is possible for E1-induced arcs inside transformers to damage transformers irrespective of relay failure. In general, since sequential shutdown is not required, one device per relay is a reasonable rule of thumb. A properly functioning relay has a reasonable chance of protecting the device; an improperly functioning one will probably result in some level of damage in an ensuing system collapse. The level of damage depends on the failure mode. The Commission-sponsored tests were focused on determining the thresholds for damage. EMP threat levels are expected to exceed these thresholds.

### **Test Results**

The EMP Commission conducted both free-field and cable current injection simulation testing. The Commission took the basic stance in its testing program that testing would determine the thresholds at which substantial failure rates (either temporary or permanent) commenced to appear. These, in turn, were used to index attack severities at which the corresponding U.S. infrastructures would be seriously compromised or failed. The Commission's test experience — massively supplemented by that of other U.S. Government operations — was that failure rates typically increased rapidly with peak field amplitude, once a threshold had been attained at which failure or disruption appeared at all. The rationale for such threshold determining testing was that abrupt and synchronized loss of only a few percent of items such as electric power system relays would have grave impacts on the functionality of the system containing such items. This is much like the effect that a few percent of vehicles on a freeway that become disabled would have, producing a serious deleterious impact on the flow of traffic.

A crude rule of thumb was that roughly a factor-of-ten increase in damage effects might be expected when the peak field amplitude was doubled; the exact scaling relation naturally varied from one device type to another and also had very substantial dependence on the frequency content of the pulse, which however, the Commission testing program explored only slightly.

Based on the testing and analysis outlined in this chapter, we estimate that a substantial and highly significant fraction of all control and protective systems within the EMP-affected area will experience some type of impact. As the test results were briefed to industry experts at NERC and the Argonne National Laboratory, it became apparent to the Commission that even minor effects noted during the testing could have significant impacts on the processes and equipment being controlled.

### ***Free-Field Testing***

EMP free-field simulation testing was conducted using a bounded wave simulator (see **figure 2-4**). The testing was conducted in three phases.

Phase I was dedicated to evaluating the so-called transfer response for the various test systems. This is a measure of the coupling strength of the external perturbation to the test



system and provides insight into the expected fraction of the energy in an EMP field that may be deposited into the exposed electronic device. Induced current transients were measured on all the accessible cables of the control systems and measurements were made at the lowest field levels produced by the simulator to minimize the electrical stress on the exposed equipment. Phases II and III of the testing program were focused on obtaining data on fragilities, that is, on identifying the thresholds for induced malfunction or damage response in the tested equipment. A total of eight steps were selected that



**Figure 2-4. EMP Simulator**

gradually increased the electrical stress on the control systems. During this testing, all systems were operational with diagnostics and checkouts run at the conclusion of each simulated EMP exposure.

The simulation testing provided an opportunity to observe the interaction of the electromagnetic energy with equipment in an operational mode. Observed effects can be related to the system response in more realistic scenarios through analysis based on coupling differences between the simulated and real-world cases. Since the simulation is not perfect — the pulse length is too long and the test volume too small to capture the longer cable run couplings to be found in a real environment — post test analysis and engineering judgment is required to relate the test results to expected SCADA vulnerabilities in a true EMP event.

There is also no pretense that any test program could possibly do more than selectively sample the wide variety of installed SCADA systems. The choice of representative test systems was guided by findings from previous infrastructure site surveys, by solicited recommendations from industry groups such as the NERC, and by conducting a review of several market surveys.

In the end, four separate control systems were acquired for testing. These systems were representative of those found in power transmission, distribution, power generation, and oil and gas distribution for fueling power plants.

A key observation from this test program is that a wide variety of SCADA, DCS, and PLC malfunctions resulted when exposed to simulated threshold level EMP environments. These ranged from electronic upset of equipment, which might be repaired by

either reboot or recycle to physical damage that required the actual replacement of the affected hardware.

The response of the control systems tested varied from system to system as well as from subsystem to subsystem. For example, a unit consisting of multiple input/output ports (or subsystems) connected to a variety of field or communications devices had some ports experience upsets, some experience physical damage, and some experience no effect, all in the same simulation event.

As an example, at relatively low electromagnetic stress levels, a portion of a DCS process controller provided false indications of the process status. An operator interface indicated a switch was on when in actuality it had been turned off, while internal voltage and temperature were reported as out of their normal operating ranges when they were actually normal. These effects were significant because they occurred most frequently on control systems used in SCADA applications, which are geographically dispersed. Correcting these malfunctions typically had to be performed manually at the device location. This approach would greatly complicate the recovery process for geographically distributed systems.

In addition to false readings from the sensors, direct malfunctions of some tested control elements were also noted. Additional control element effects included the failure of pressure transmitters, which included both physical damage and loss of calibration data required to indicate proper readings.

Control systems often rely on Ethernet for communications to the man-machine interface as well as communications between controllers in dispersed systems. Communications systems based on Ethernet components similar to those found in PC networking systems suffered substantial degradation and damage effects when illuminated by the simulated albeit low-level EMP pulse. These damage effects are significant since they require the systems to be physically repaired or replaced in order to restore the normal communications capabilities.

Many of the effects noted in the previous paragraphs are attributed to the coupling to the wires and cables interconnecting the systems. The level of this coupling scales roughly with the length of the wire. As a general rule, the larger the transients are in the coupling lines, the more damaging they are to electronics equipment. It is therefore important to consider the transients that might be induced if a more distributed system encounters the same EMP electromagnetic energy. One way to address this concern is to perform cable coupling analysis. This was done as part of the current injection test program in order to relate the susceptibility levels of electronic equipment to the EMP threat.

At the system level, 100 percent of the control systems were affected at times. This is highly relevant to the prospect of system collapse and scope of the problem of restoration. This is more difficult to quantify at the subsystem level due to the sheer number of subsystems associated with each system. Translation to real world conditions must be tempered in cases where the control systems are located in structures that provide electromagnetic shielding of the incident EMP energy, but few of these exist in practice.

### ***Current Injection Testing***

Current injection testing was typically done by introducing transient voltage waveforms on a cable leading to the equipment under test. Depending on its load and that of the test generator, current was delivered to the test object. All of the electronics found in the power system is developed using a national (ANSI/IEEE) or international (IEC) standard

---

for a series of electromagnetic compatibility (EMC) waveforms that are representative of the transients observed during normal operation. One waveform that is commonly tested is known as the electrical fast transient (EFT). It has a rise time of 5 ns and a pulse width of 50 ns. By coincidence, this is very similar to the type of waveform coupled to cables by E1.

The objective of this testing was to determine at what level each type of equipment fails to operate normally and also to determine when operator intervention is necessary for the equipment to operate normally. Most of the equipment tested had multiple cable connections, covering different functions (power, signal, communications, etc.). These were all tested.

Given the levels of voltage in which the equipment malfunctioned, a separate effort was performed to compute the coupling of the incident E1 to cables with various lengths and orientations. For the long, exposed cables found in transmission substations, it was found that the induced voltage could exceed 20 kV under many circumstances.

In addition to free-field testing, the Commission sponsored a current injection testing program. The test program was representative in the sense that exemplars of most functional components were tested. Due to expense and time constraints, typically only one or two vendors' equipment was tested, and only one or two samples of a type were tested. The types of equipment tested and results brief are described in the following paragraphs:

***Electro-mechanical relays.*** These are the old-fashioned devices that contain no integrated circuits but function using high-power relays. They are still used in about 50 percent of applications, but that share is continuing to decline. As expected, these are immune to EMP upset up to the highest levels tested.

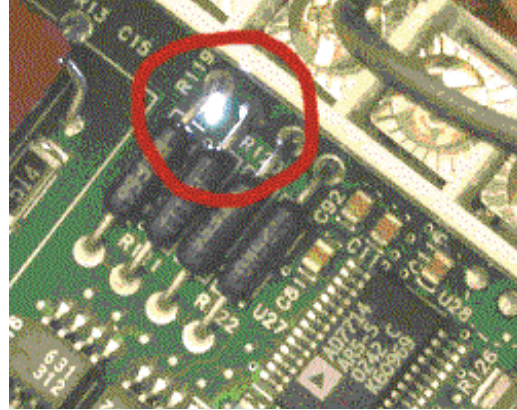
***Distribution line insulators.*** Earlier studies have indicated low vulnerability for these simple devices. The Commission-sponsored tests on a variety of 15kV class pin and suspension insulators indicate that there is a higher vulnerability than previously thought. New tests performed with the power on found that some insulators were destroyed due to the current following the path of the E1-induced arc. Statistical testing was not performed, so it is not clear what percentage of insulators will behave in this fashion; however, it is clear that power-on testing should be performed in the future to better understand this effect.

***Electronic protective relays.*** These devices (see **figure 2-5**) are the essential elements preserving high-value transmission equipment from damage during geomagnetic storms and other modes of grid collapse. Fortunately, these test items were the most robust of any of the electronic devices tested. However, test agencies reported that they are subject to upset at higher levels of simulated EMP exposure. We believe that altering the deployment configurations can further ameliorate the residual problems.



**Figure 2-5. Test Item: Electronic Relay**

*Programmable logic controllers and digital control systems.* These units are most commonly found in industrial settings and in particular are extensively used in power plants. They are subject to upset and damage at moderate levels of EMP assault (see **figure 2-6**). The circuit board pictured is from a typical PLC unit and is exhibiting a damaging short-circuit flashover during EMP Commission-sponsored testing.



**Figure 2-6. Flashover Observed During Injection Pulse Testing**

*General-purpose desktop computers and SCADA remote and master terminal units.* These were the most susceptible to damage or upset of all the test articles. Unlike the other kinds of devices tested, several different models and vintages were examined. The RS-232 ports were found to be particularly susceptible, even at very low levels of EMP stress.

With the exception of the RS-232 connections, all of the electronic devices that were tested performed up to the manufacturer's claimed levels for electromagnetic compatibility. Thus, the international standards to which the manufacturers subscribe are being met. Unfortunately the induced E1 stress is higher than the standards for normal operation.

The net result of this testing provides evidence that the power grid is also vulnerable to collapse due to the E1 component of an EMP assault, primarily through the upset and damage of the soft computer systems that are in common use. This however suggests that operational performance can be considerably enhanced at modest cost by attending to installation and configuration issues.

### **Historical Insights**

To provide insight into the potential impact of EMP-induced electronic system malfunctions, the Commission evaluated previous large service failure events. In these cases, similar (and less severe) system malfunctions have produced consequences in situations that were far too complex to predict using a model or analysis.

Another important observation is that these situations are seldom the result of a single factor but rather a combination of unexpected events, which are easily related to the impact only in hindsight. This is not surprising given the complexity, interdependency, and size of the systems involved. It is important to note that historical examples, while necessary for the insight they provide into the dependence of a functioning modern infrastructure on its automated control systems, do not remotely capture the scale of the expected EMP scenario. In an EMP event, it is not one or a few SCADA systems that are malfunctioning (the typical historical scenario) but very large numbers, hundreds or even thousands over a huge geographic area with a significant fraction of those rendered permanently inoperable until replaced or physically repaired. Critically, the systems that would identify what components are damaged and where they are located are also unavailable in many instances.

*Hurricane Katrina, August 2005.* Hurricane Katrina, one of the worst U.S. natural disasters ever, caused a widespread, multi-state blackout that lasted for a prolonged period, with catastrophic consequences for the afflicted region. The Katrina blackout was



a major factor in the failure of police, emergency and rescue services during the hurricane, which killed 1,464 people. The blackout caused gas stations to cease operating, paralyzing transportation and greatly impeding evacuation efforts. The Katrina blackout, which afflicted the region for weeks and lasted for months in some localities, so severely impeded recovery efforts that even today, 3 years later, New Orleans and its vicinity is still far from being fully recovered.

*August 14, 2003, Blackout.* The August 14 blackout was precipitated by a single line failure in one control area. It eventually affected nine control areas over a period of several hours, with rapidly spreading cascades of outage over the last 30 minutes. The extent of the blackout was exacerbated by deficiencies in specific practices, equipment, and human decisions. Initial retrospectives have focused on three likely contributory causes:

- ◆ Inadequate situational awareness at First Energy Corporation (FEC)
- ◆ FEC's failure to adequately manage tree growth in its transmission rights-of-way
- ◆ Failure of the interconnected grid's reliability organizations to provide effective diagnostic support.

The inadequate situational awareness and failure to provide effective diagnostic support are closely aligned to the computer and network effects that showed damage and upset during EMP testing. Additionally, new causal features (not common to other blackout incidents) of the August 14 blackout include inadequate interregional visibility over the power system, dysfunction of a control area's SCADA system, and lack of adequate backup capability to that system. Thus, all of the factors involved in the August 14 blackout are expected to be present in control areas impacted by an EMP event, but to a far greater extent. Therefore, an event as large as the ultimate August 14 blackout could be part of an initial EMP impact but multiplied several times over a contiguous geographical and system area. If this effect overlapped the Eastern and Western Interconnections, there is the increased probability that both interconnections could collapse.

*Western States Blackout.* The 1996 Western States blackout occurred when an electrically loaded transmission line sagged onto a tree and caused a short. This type of event is not uncommon, especially in the heavily treed areas of the Western Interconnect. At about the same time, a second line tripped (opened) due to improper protective relay activation. The tripping of the two transmission lines, coupled with a heavy electrical load on these lines and the thin margins on the transmission system, triggered the widespread outage through cascading failure. An EMP event could be expected to result in the loss of numerous transmission lines at once, not just the two cited in this case.

*Geomagnetic Storms.* Probably one of the most famous and severe effects from solar storms occurred on March 13, 1989. On this day, several major impacts occurred to the power grids in North America and the United Kingdom. This included the complete blackout of the Hydro-Quebec power system and damage to two 400/275 kV autotransformers in southern England. In addition, at the Salem nuclear power plant in New Jersey, a 1200 MVA, 500 kV transformer was damaged beyond repair when portions of its structure failed due to thermal stress. The failure was caused by stray magnetic flux impinging on the transformer core. Fortunately, a replacement transformer was readily available; otherwise the plant would have been down for a year, which is the normal delivery time for larger power transformers. The two autotransformers in southern England were also damaged from stray flux that produced hot spots, which caused significant gassing from the breakdown of the insulating oil.

The blackout of the Hydro-Quebec system was caused when seven static voltage-amps reactive (VAR) compensators (SVC) tripped and shut down due to increased levels of harmonics on the power lines. The loss of the seven SVCs led to voltage depression and frequency increase on the system, which caused part of the Quebec grid to collapse. Soon afterwards, the rest of the grid collapsed because of the abrupt loss of load and generation. The blackout took less than 90 seconds to occur after the first SVC tripped. About 6 million people were left without power for several hours and, even 9 hours later, there were still 1 million people without power.

Geomagnetic storms represent an approximation to an E3-induced voltage effect. The experience to date is of events that may be orders of magnitude smaller in scope and less severe than that expected from an EMP — although the Commission has also investigated the impact of a 100-year superstorm. The induced geomagnetic superstorm currents in the transmission lines will cause hundreds of high voltage transformers to saturate, creating a severe reactive load in the power system leading to voltage collapse in the affected area and damage to elements of the transmission system. The nature of this threat did not allow for experimental testing of the E3 effect, so this historical record is the best information on the effect.

### **Distinctions**

Past electric power blackouts provide a baseline for assessing the impact of an EMP attack on the power grid as discussed previously. However, there are several important factors that distinguish the EMP collapse scenario from these historical experiences.

- ◆ In the historical power system outages, only one or a few critical elements within an entire system have been debilitated. For example, a power generation facility may trip because a surge of current is unexpectedly presented through a fault from a particular load. Yet a substantial portion of the system may well be rendered out of service as the disruption triggers a series of cascading failures, each instigating the next failure (e.g., first a generator trips, then the frequency sags, and a load trips off or a transmission line trips out with its associated loads, which in turn causes the frequency to overrun and another generator trips out, and it continues to oscillate until the interconnected system comes down.) In the case of an EMP attack, elements within many critical facility components are likely to be damaged or disrupted simultaneously over a relatively broad geographic area, thus creating an almost certain cascading collapse of the remaining elements. Similarly, while lightning might strike a single plant, transmission line, or large load causing it to trip out, lightning has not hit multiple locations spread over a very wide area of the system with sufficient intensity and hitting all simultaneously to the extent that would be representative of an EMP attack.
  - ◆ During historical outages, the telecommunications system and associated control systems have continued to function. This provides the system operators with eyes and ears to know what was damaged, where damage occurred and in some cases the range of damage. While the power system may still come down, it is more possible to take protective measures to minimize damage and impact in order to effectuate rapid restoration. The communications and control systems' functionality are at high risk of disruption and damage themselves during an EMP attack. A minimum communications capability is needed to support immediate responses, to isolate parts for continued operation, and to implement necessary measures to restore the electrical system.
  - ◆ In the early stages of the EMP attack, even before the disruptions could be sensed and trips could occur that would lead to collapse, some or many of the protective devices
-



will be damaged that have ensured critical system components are safe to allow fast recovery. As a result, some and perhaps much of the electrical system would not be able to protect itself from the effects of multiple simultaneous and cascading failures. Widespread damage to the generation, transmission, and distribution infrastructures and equipment are probable. Rather than simply restoring power to an intact infrastructure with only a very few damaged components, the recovery task would be to replace an extensively damaged system under very difficult and decaying circumstances and then proceeding to restoration.

- ◆ The control systems would be damaged to some extent as opposed to remaining fully operational as in historical outages. The operations and dispatch centers where the vast interconnected system is controlled and managed would probably have damaged and disrupted components, the readings from the system would be fragmented and in many cases false or nonexistent, and communication by whatever means would be difficult to impractical to impossible. Control and knowledge would range from unreliable at best to simply nonexistent. Finding what and where damage has occurred and getting it repaired would be very problematic in any reasonable time frame, even within the control centers themselves, let alone out over the vast network with millions of devices.
- ◆ Skilled labor for a massive and diverse repair effort is not currently available if allocated over a large geographic area with great numbers of components and devices to check and repair where necessary. This scope of damage could cover perhaps 70 percent or possibly more of the continental United States as well as a significant part of Canada's population. This is far too large to bring in the limited skilled labor from very distant points outside the affected area in any reasonable time, even if one could coordinate them and knew where to send them, and they had the means to get there. Thus the extensive support from nearby fringe areas used so effectively in historical outages is likely to be unavailable as a practical matter as they themselves would be affected. The blackout resulting from Hurricane Katrina, an event comparable to a small EMP attack, overtaxed the ability of the Nation to quickly restore electric power, a failure that contributed to the slow recovery of the afflicted region.
- ◆ Other infrastructures would be similarly impacted simultaneously with the electrical system such as transportation, communication, and even water and food to sustain crews. The ability to find and get spare parts and components or purchase services would be severely hampered by lack of normal financial systems in addition to communication, transportation, and other factors. The Hurricane Katrina blackout caused precisely such problems.
- ◆ Fuel supplies for the power generation would be interrupted. First, the SCADA and DCS systems used in delivery of the fuel would be adversely impacted. In addition, much of the fuel supply infrastructure is dependent upon the electrical system. For example, natural gas-fired plants (which make up such a large share of the domestic generation) would be rendered inoperable since their fuel is delivered just in time for use. Coal plants have stockpiles that variously might be adequate for a week to a month. The few remaining oil-fired plants similarly have a limited storage of fuel. Nuclear plants would reasonably be expected to still have fuel but they would have to forego protective regulations to continue to operate. Many renewable fueled resources would still have their fuel supply but EMP effects on controls may still render them inoperable.

It is not possible to precisely predict the time to restore even minimal electrical service due to an EMP eventuality given the number of unknowns and the vast size and complexity of the system with its consequent fragility and resiliency. Expert judgment and rational extrapolation of models and predictive tools suggest that restoration to even a diminished but workable state of electrical service could well take many weeks, with some probability of it taking months and perhaps more than a year at some or many locations; at that point, society as we know it couldn't exist within large regions of the Nation. The larger the affected area and the stronger the field strength from the attack (corollary to extent of damage or disruption), the longer will be the time to recover. Restoration to current standards of electric power cost and reliability would almost certainly take years with severe impact on the economy and all that it entails.

### **Strategy**

The electrical system must be protected against the consequences of an EMP event to the extent reasonably possible. The level of vulnerability and extreme consequence combine to invite an EMP attack. Thus reduction of our vulnerability to attack and the resulting consequences reduces the probability of attack. It is also clear the Cold War type of deterrence through mutual assured destruction is not an effective threat against many of the potential protagonists, particularly those who are not identifiable nation-states. The resulting strategy is to reduce sharply the risk of adverse consequences from an EMP attack on the electrical system as rapidly as possible. The two key elements of the mitigation strategy for the electrical system are protection and restoration.

The initial focus for reducing adverse consequences should be on the restoration of overall electrical system performance to meet critical, if not general, societal needs. The focus should be on the system as a whole and not on individual components of the system. Timely restoration depends on protection, first of high-value assets, protection necessary for the ability to restore service quickly to strategically important loads, and finally protection as required to restore electrical service to all loads. The approach is to utilize a comprehensive, strategic approach to achieve an acceptable risk-weighted protection in terms of performance, schedule, timing, and cost. The effort will include evolution to greater and greater levels of protection in an orderly and cost-effective manner consistent with the anticipated threat level. Where possible, the protection also will enhance normal system reliability and, in so doing, provide great service to society overall.

There is a point in time at which the shortage or exhaustion of critical items like emergency power supply, batteries, standby fuel supplies, replacement parts, and manpower resources which can be coordinated and dispatched, together with the degradation of all other infrastructures and their systemic impact, all lead toward a collapse of restoration capability. Society will transition into a situation where restoration needs increase with time as resources degrade and disappear. This is the most serious of all consequences and thus the ability to restore is paramount.

### **Protection**

It is not practical to try to protect the entire electrical power system or even all high-value components from damage by an EMP event. There are too many components of too many different types, manufactures, ages, and designs. The cost and time would be prohibitive. Widespread collapse of the electrical power system in the area affected by EMP is virtually inevitable after a broad geographic EMP attack, with even a modest number

of unprotected components. Since this is a given, the focus of protection is to retain and restore service to critical loads while permitting relatively rapid restoration.

The approach to protection has the following fundamental aspects. These will collectively reduce the recovery and restoration times and minimize the net impact from assault. All of this is feasible in terms of cost and timing if done as part of a comprehensive and reasonable response to the threats, whether the assault is physical, electromagnetic (such as EMP), or cyber.

1. Protect high-value assets through hardening. Hardening, providing for special grounding, and other schemes are required to assure the functional operation of protection equipment for large high-value assets such as transformers, breakers, and generators and to so protect against sequential, subsequent impacts from E2 and E3 creating damage. Protection through hardening critical elements of the natural gas transportation and gas supply systems to key power plants that will be necessary for electrical system recovery is imperative.
  2. Assure there are adequate communication assets dedicated or available to the electrical system operators so that damage during system collapse can be minimized; components requiring human intervention to bring them on-line are identified and located; critical manpower can be contacted and dispatched; fuel, spare parts and other commodities critical to the electrical system restoration can be allocated; and provide the ability to match generation to load and bring the system back on line.
  3. Protect the use of emergency power supplies and fuel delivery, and importantly, provide for their sustained use as part of the protection of critical loads, which loads must be identified by government but can also be assured by private action. Specifically:
    - Increase the battery and on-site generating capability for key substation and control facilities to extend the critical period allowing recovery. This is relatively low cost and will improve reliability as well as provide substantial protection against all forms of attack.
    - Require key gasoline and diesel service stations and distribution facilities in geographic areas to have at-site generation, fueled off existing tanks, to assure fuel for transportation and other services, including refueling emergency generators in the immediate area.
    - Require key fueling stations for the railroads to have standby generation, similar to that required for service stations and distribution facilities.
    - Require the emergency generator start, operation, and interconnection mechanisms to be EMP hardened or manual. This will also require the ability to isolate these facilities from the main electrical power system during emergency generation operation and such isolation switching must be EMP hardened.
    - Make the interconnection of diesel electric railroad engines and large ships possible and harden such capability, including the continued operation of the units.
    - The Government must determine and specify immediately those strategically important electrical loads critical to the Nation to preserve in such an emergency.
  4. Separate the present interconnected systems, particularly the Eastern Interconnection, into several nonsynchronous connected subregions or electrical islands. It is very important to protect the ability of the system to retain as much in operation as possible through reconfiguration particularly of the Eastern Connected System into a number of nonsynchronous connected regions, so disruptions will not cascade beyond those EMP-disrupted areas. Basically, this means eliminating total NERC region service loss, while at the same time maintaining the present interconnection status with
-

its inherent reliability and commercial elements. This is the most practical and easiest way to allow the system to break into islands of service and greatly enhance restoration timing. This will not protect most within the EMP-insult area, but it should increase the amount of viable fringe areas remaining in operation. This is fiscally efficient and can leverage efforts to improve reliability and enhance security against the broader range of threats, not only EMP. It also can be beneficial to normal system reliability.

5. Install substantially more black start generation units coupled with specific transmission that can be readily isolated to balancing loads. The NERC regions now do surveys of available black start and fuel switchable generation. Requiring all power plants above a certain significant size to have black start or fuel-switching capability (with site-stored fuel) would be a very small added expense that would provide major benefits against all disruptions including nonadversarial ones. Black start generator, operation, and interconnection mechanisms must be EMP hardened or be manual without microelectronic dependence. This also will require the ability to isolate these facilities from the main electrical power system during emergency generation operation and that isolation switching is EMP hardened. In addition, sufficient fuel must be provided, as necessary, to substantially expand the critical period for recovery.
6. Improve, extend, and exercise recovery capabilities. Develop procedures for addressing the impact of such attacks to identify weaknesses, provide training for personnel and develop EMP response training procedures and coordinate all activities and appropriate agencies and industry. While developing response plans, training and coordination are the primary purpose.

### ***Recovery and Restoration***

The key to minimizing catastrophic impacts from loss of electrical power is rapid restoration. The protective strategy described is aimed primarily at preserving the system in a recoverable state after the attack, maintaining service to critical loads, and enhancing recovery.

The first step in recovery is identifying the extent and nature of the damage to the system and then implementing a comprehensive plan with trained personnel and a reservoir of spare parts to repair the damage. Damage is defined as anything that requires a trained person to take an action with a component, which can include simply rebooting all the way to replacing major internal elements of the entire component. A priority schedule for repair of generation, transmission, and even distribution is necessary since resources of all types will be precious and in short supply should the EMP impact be broad enough and interdependent infrastructures be adversely impacted (e.g., communication, transportation, financial and life-supporting functions).

Restoration is complicated in the best of circumstances, as experienced in past black-outs. In the instance of EMP attack, the complications are magnified by the unprecedented scope of the damage both in nature and geographical extent, by the lack of information post attack, and by the concurrent and interrelated impact on other infrastructures impeding restoration.

Restoration plans for priority loads are a key focus. Widely scattered or single or small group loads are in most cases impractical to isolate and restore individually given the nature of the electrical system. These are to be served first through the emergency power supply aspects identified in the Protection section. Restoration of special islands can,

however, be made practical by the nonsynchronous connected subregions if they are identified by the Government as necessary very far in advance of any assault. Otherwise, the system's resources and available personnel will need to act expeditiously to get as many islands of balanced load and generation back into operation. This will begin by system operators identifying those easiest to repair (normally the least damaged) and restore them first. As these stabilize, the system recovery will flow outward as, increment by increment, the system is repaired and brought back in service. It is much more feasible and practical to restore by adding incrementally to an operating island rather than black starting the recovery for an island.

Balancing an isolated portion of generation and load first, and then integrating each new increment is a reasonably difficult and time-consuming process in the best of circumstances. In an EMP attack with multiple damaged components, related infrastructure failures, and difficulty in communications, restoring the system could take a very long time unless preparatory action is taken.

Generating plants have several advantages over the widely spread transmission network as it relates to protection and restoration from an EMP event. The plant is one complete unit with a single DCS control network. It is manned in most cases so operators and maintenance personnel are immediately available and on site. The operating environment electronically requires a level of protection that may provide at least a minimal protection against EMP. Nevertheless, it is important to harden critical controls sufficiently to enable manual operation at a minimum. Providing for at-site spares to include the probably needed replacements for control of operation and safety would be straightforward and not expensive to accomplish, thus assisting rapid restoration of capability.

As controls and other critical components of the electrical transmission and generation system suffer damage, so do similar components on the production, processing, and delivery systems providing fuel to the electric generators. Restoration of the electrical power system is not feasible on a wide scale without a parallel restoration of these fuel processing and delivery systems.

Hydropower, wind, geothermal, and solar power each has a naturally reoccurring fuel supply that is unaffected by EMP. However, the controls of these plants themselves are subject to damage by EMP at present. In addition, only hydropower and geothermal have controllable fuel (i.e. they can operate when needed versus wind and solar that operate when nature provides the fuel just-in-time). As a practical matter, only hydropower is of sufficient size and controllability in some regions to be a highly effective resource for restoration, such as the Pacific Northwest, the Ohio/Tennessee valley, and northern California. Beyond the renewable resources, coal and wood waste plants typically have significant stockpiles of fuel so the delay in rail and other delivery systems for a couple of weeks and in some instances up to a month is not an issue for fuel. Beyond that, rail and truck fuel will be needed and delivery times are often relatively slow, so the delivery process must start well before the fuel at the generator runs out.

Operating nuclear plants do not have a fuel problem per se, but they are prohibited by regulation from operating in an environment where multiple reliable power supply sources are not available for safe shutdown, which would not be available in this circumstance. However, it is physically feasible and safe for nuclear plants to operate in such a circumstance since they all have emergency generation at site. It would simply have to be fueled sufficiently to be in operation when the nuclear plant is operating without external



electrical supply sources. Nuclear power backup would need to be significantly expanded. Natural gas-fired power plants are very important in restoration because of their inherent flexibility and often their relatively small size, yet they have no on-site fuel storage and are totally dependent upon the natural gas supply and gas transportation system which are just in time for this purpose. Therefore, the natural gas fuel delivery system must be brought back on-line before these power plants can feasibly operate. It is operated largely with gas turbines of its own along the major pipelines. The key will be to have the protection, safety, and controls be hardened against EMP.

Recovery from transmission system damage and power plant damage will be impeded primarily by the manufacture and delivery of long lead-time components. Delivery time for a single, large transformer today is typically one to two years and some very large special transformers, critical to the system, are even longer. There are roughly 2,000 transformers in use in the transmission system today at 345 kV and above with many more at lesser voltages that are only slightly less critical. No transformers above 100 kV are produced in the United States any longer. The current U.S. replacement rate for the 345 kV and higher voltage units is 10 per year; worldwide production capacity of these units is less than 100 per year. Spare transformers are available in some areas and systems, but because of the unique requirements of each transformer, there are no standard spares. The spares also are owned by individual utilities and not generally available to others due to the risk over the long lead time if they are being used. Transformers that will cover several options are very expensive and are both large and hard to move. NERC keeps a record of all spare transformers.

Recovery will be limited by the rate of testing and repair of SCADA, DCS, and PLC and protective relay systems. With a large, contiguous area affected, the availability of outside assistance, skilled manpower, and spares may well be negligible in light of the scope of the problem. Information from power industry representatives enables us to place some limits on how long the testing and repair might take. Determining the source of a bad electrical signal or tiny component that is not working can take a long time. On the low side, on-site relay technicians typically take three weeks for initial shakedown of a new substation. Simply replacing whole units is much faster, but here too, inserting new electronic devices and ensuring the whole system works properly is still time consuming. It must be noted that the substations are typically not manned so skilled technicians must be located, dispatched, and reach the site where they are needed. Many of these locations are not close to the technicians. It is not possible to readily estimate the time it will take in the event of an EMP attack since the aftermath of an EMP attack would not be routine and a certain level of risk would likely be accepted to accelerate return to service. It seems reasonable, then, to estimate an entire substation control system recovery time to be at least several days, if not weeks. This assumes that the trained personnel can reach the damaged locations and will be supported with water, food, communication, spare parts, and the needed electronic diagnostic equipment.

Unlike generation, recovery of the transmission system will require off-site communications because coordination between remote locations is necessary. Communications assets used for this purpose now include dedicated microwave systems and, increasingly, cell phones and satellite systems. If faced with a prolonged outage of the telecommunications infrastructures, repairs to dedicated communication systems or establishment of new ad-hoc communications will be necessary. This might take one or more weeks and



would set a lower limit on recovery time, but it would be unlikely to affect the duration of a months-long outage.

Restoration to electrical service of a widely damaged power system is complex. Beginning with a total blackout, it requires adequate communication to match and coordinate a generating plant to a load with an interconnected transmission that normally can be isolated via switching at several substations, so it is not affected by other loads or generation. The simultaneous loss of communication and power system controls and the resulting lack of knowledge about the location of the damage all greatly complicate restoration. There are also a diminishing number of operators who can execute the processes necessary for restoration without the aid of computers and system controls.

Without communication, both voice and data links, it is nearly impossible to ascertain the nature and location of damage to be repaired, to dispatch manpower and parts, and to match generation to load. Transportation limitations further impede movement of material and people. Disruption of the financial system will make acquisition of services and parts difficult. In summary, actions are needed to assure that difficult and complex recovery operations can take place and be effective in an extraordinarily problematic post-attack environment.

The recovery times for various elements of the electrical system are estimated in the following paragraphs. These should be regarded as very rough best estimates for average cases derived from the considered judgment of several experts. These estimates are gross averages, and the situation would vary greatly from one facility to another as the situation, number of disrupted and damaged elements and the extent of preassault preparedness and training vary. In addition, the contingencies and backlogs strongly depend on the extent of such damage elsewhere and are essentially unknown. For example, fuel delivery capability is a key element. Each of the system elements — generation (including fuel delivery), transmission, distribution, and often load — must be repaired and in working order sufficient for manual control at a minimum (each element with skilled personnel all in communication with each other). Thus, the following should be occurring in parallel as much as possible, but in some instances testing of one element requires a working capability of another. The availability of spare parts and trained manpower coupled with knowledge of what to repair and where it is are critical to recovery timing. The recovery times provided below are predicated upon the assumption that the other infrastructures are operating normally. The recovery times would increase sharply with the absence of other operating infrastructures, which is likely in the EMP situation. These estimates are based upon present conditions, not what is possible if the Commission recommendations are followed.

#### *Power Plants*

- ◆ Replace damaged furnace, boiler, turbine, or generator: one year plus production backlog plus transportation backlog. It is uncertain if and to what extent damage to these elements will occur if the protection schemes are disrupted or damaged.
- ◆ Repair some equipment if spares on site exist, but repair time depends on the type of plant and personnel available at the plant at the time of the assault: two days to two weeks plus service backlog at the site or to move trained personnel from plant to plant.
- ◆ Repair and test damaged SCADA, DCS, and computer control system: three months.
- ◆ Return repaired or undamaged plant to operation, provided the major components under the first bullet are not damaged: (1) nuclear: three days provided there is an

independent power feed with enough fuel, which should be on site in such an emergency, (2) coal: two days plus black start or independent power feed, (3) natural gas: two hours to two days depending on fuel supply and black start, (4) hydro: immediate to one day, (5) geothermal: one to two days, (6) wind: immediate to one day unless each turbine requires inspection and then one or two turbines a day.

- ◆ All of the above are also contingent on the availability of fuel. Our recommendations for on-site reserves: coal: 10-30 days; natural gas: depends on whether the pipeline is operating; nuclear: 5 days to several weeks; hydro: depends on reservoir capacity available for continued use.

#### *Transmission and Related Substations*

- ◆ Replace irreparably damaged large transformers: One to two years plus production backlog plus transportation plus transportation backlog (these are very large and require special equipment to transport that may not be available in this situation).
- ◆ Repair damaged large transformer: one month plus service backlog.
- ◆ Repair manual control system: one month if adequate personnel are available.
- ◆ Establish ad hoc communications: one day to two weeks.
- ◆ Repair and test damaged protective systems: three months.
- ◆ Repair and return of substations to service are also contingent on the local availability of power. All substations have batteries for uninterrupted power, nominally enough for eight hours. Very few (about 5 percent) have on-site emergency generators. Many utilities rented emergency generators in advance of the Y2K transition. Almost all are now gone. Once the local power is gone, other emergency power often must be brought to the station for operation.
- ◆ Assuming DC terminals are manned: one week to one month depending upon damage.

#### *Distribution and Related Substations*

- ◆ Replace insulators that have flash-over damage: two to five days, unless very widespread and then weeks.
- ◆ Replace service transformers: two to five days unless very widespread and then weeks.
- ◆ Repair time depends on the number of spares, available crews that perform the repairs, and equipment.
- ◆ Note that the load on the end of the distribution may have some disruption that needs repair as well.

Starting an electrical power system from a fully down and black system requires one of the following two approaches. (1) At the margin of the outage, an operating electrical system is running at proper frequency with balanced load to generation, and this system can be interconnected to the fringe of the black portion of the system. The newly interconnected portion, the portion being restored, must be able to sequentially (in increments or simultaneously) bring on load and generation to keep the now larger portion of the system in sufficient frequency balance so the entire system, new and old, does not collapse. Then another increment is integrated into the operating system and so on. As the portion that is operating in balance becomes larger and more flexible, the increments that are able to be added become larger as well, since the operating system can absorb more and maintain stability. This is how historical outage areas are predominantly restarted. (2) There is generation that can be black started. This means starting a generator without an external power source, such as hydroelectric or diesel generation. To do this, the genera-

tion has to be synchronized on line, and a load has to be matched to the generation as it comes on line. That requires that a transmission link between the generation and the load be put in service. Yet the transmission link also must be segregated from the rest of the system, or the load hanging on it would be too large. Both approaches require that the increment of the system being re-energized to be fully functional (repaired) and communication established between the generation and load, including any substation or switchyard between the two. Importantly, it requires skilled personnel to execute the restoration manually.

The generation must have sufficient fuel to accommodate the load being met in balance. Water behind a hydroelectric facility may be limited and certainly the diesel fuel is likely to be limited. Thus the startup must be done carefully because failures could render the black start inoperable as it runs out of fuel or depletes the battery. Normally, in this type of situation, the diesel or small hydro is used primarily to start up a larger generator of a size that can carry the necessary load increment. This larger generator must be fueled, which can be a complication as discussed elsewhere in this chapter.

Under deregulation, the disconnection (in the business sense) of transmission from generation that has been occurring in the U.S. electrical power business creates a problem for black start recovery. There are risks involved in returning a plant to operation and costs for the needed repairs. Questions about who will pay whom and who will follow whose direction is not easy to answer, even with everybody wanting to cooperate. Under the historic utility monopolies, the generation and the transmission assets had a common owner, so these matters were handled within a single organization. Now, coordination with independent power producers is nearly unenforceable other than through heavy government emergency powers noting that power producers and owners want indemnification before assuming risk. Therefore some degree of command authority is required for coordination, assessment, and acceptance of risk of damage and financial settlement of losses.

The time to integrate sufficient portions of a black region of the system using the fringe approach is reasonably short if the outage area is small in relation to the operating area as has been seen in past outage conditions. In the case of EMP, where the outage area is likely to be much larger than the fringe area or there is no fringe area, restoration of even parts will be measured in weeks to months. If communication is difficult to nonexistent, restoration can take much longer.

### ***Mitigation of Adverse Consequences***

By protecting key system components, structuring the network to maximize fringe service, through the nonsynchronous interconnections, expanding the black start and system emergency power support, creating comprehensive recovery plans for the most critical power needs, and providing adequate training of personnel, the risk of catastrophic impact to the Nation can be significantly reduced. The mitigation plan must be jointly developed by the Federal Government and the electric power industry, instilled into systems operations, and practiced to maintain a ready capability to respond. It must also be fully coordinated with the interdependent infrastructures, owners, and producers.

The continuing need to improve and expand the electric power system as a normal course of business provides an opportunity to judiciously improve both security and reliability in an economically acceptable manner — provided that technically well-informed decisions are made with accepted priorities. There are a wide variety of potential threats

besides EMP that must be addressed, which can have serious to potentially catastrophic impacts on the electrical system. Common solutions must be found that resolve these multiple vulnerabilities as much as possible. For example, in the course of its work, the Commission analyzed the impact of a 100-year solar storm (similar to E3 from EMP) and discovered a very high consequence vulnerability of the power grid. Steps taken to mitigate the E3 threat also would simultaneously mitigate this threat from the natural environment. Most of the precautions identified to protect and restore the system from EMP will also apply to cyber and physical attacks. The Commission notes that the solutions must not seriously penalize our existing and excellent system but should enhance its performance wherever possible.

The time for action is now. Threat capabilities are growing and infrastructure reinvestment is increasingly needed which creates an opportunity for the investment to serve more than one purpose. Government must take responsibility for improvements in security. As a general matter, improvements in system security are a Government responsibility, but it may also enhance reliability if done in certain ways. For example, providing spare parts, more black start capability, greater emergency back-up, nonsynchronous interconnections, and more training all will do so. Yet, EMP hardening components will not increase reliability or enhance operation. Conversely improving reliability does not necessarily improve security, but it may if done properly. For example, adding more electronic controls will not enhance EMP security, but electronic spare parts and more skilled technicians will help improve security and reliability. Finding the right balance between the utility or independent power producer's service and fiscal responsibility with the Government's security obligation as soon as possible is essential, and that balance must be periodically (almost continuously) reexamined as technology and system architecture changes.

## **Recommendations**

EMP attack on the electrical power system is an extraordinarily serious problem but one that can be reduced below the level of a catastrophic national consequence through focused effort coordinated between industry and government. Industry is responsible for assuring system reliability, efficiency, and cost effectiveness as a matter of meeting required service levels to be paid for by its customers. Government is responsible for protecting the society and its infrastructure, including the electric power system. Only government can deal with barriers to attack — interdiction before consequence. Only government can set the standards necessary to provide the appropriate level of protection against catastrophic damage from EMP for the civilian sector. Government must validate related enhancements to systems, fund security-only related elements, and assist in funding others.

It must be noted, however, that the areas where reliability and security interact represent the vast majority of cases. The power system is a complex amalgamation of many individual entities (public, regulated investor-owned, and private), regulatory structures, equipment designs, types and ages (with some parts well over one hundred years old and others brand new). Therefore, the structure and approach to modifications must not only recognize the sharply increased threat from EMP and other forms of attack, but improvements must be accomplished within existing structures. For example, industry investment to increase transmission capacity will improve both reliability and system security during the period when transmission system operating margins are increased.

The Commission concluded that mitigation for a majority of the adverse impact to the electrical system from EMP is reasonable to undertake in terms of time and resources. The specific recommendations that follow have been reviewed with numerous entities with responsibility in this area. The review has been in conceptual terms, with many of the initiatives coming from these parties, but the recommendations are the Commission's responsibility alone. The activities related to mitigation of adverse impacts on fuel supply to electric generation are more fully discussed in a separate chapter of this report.

### ***Responsibility***

As a result of the formation of Department of Homeland Security (DHS) with its statutory charter for civilian matters, coupled with the nature of EMP derived from adversary activity, the Federal Government, acting through the Secretary of Homeland Security, has the responsibility and authority to assure the continuation of civilian U.S. society as it may be threatened through an EMP assault and other types of broad scale seriously damaging assaults on the electric power infrastructure and related systems.

It is vital that DHS, as early as practicable, make clear its authority and responsibility to respond to an EMP attack and delineate the responsibilities and functioning interfaces with all other governmental institutions with individual jurisdictions over the broad and diverse electric power system. This is necessary for private industry and individuals to act to carry out the necessary protections assigned to them and to sort out liability and funding responsibility. DHS particularly needs to interact with FERC, NERC, state regulatory bodies, other governmental institutions at all levels, and industry in defining liability and funding relative to private and government facilities, such as independent power plants, to contribute their capability in a time of national need, yet not interfere with market creation and operation to the maximum extent practical.

DHS, in carrying out its mission, must establish the methods and systems that allow it to know, on a continuous basis, the state of the infrastructure, its topology, and key elements. Testing standards and measurable improvement metrics should be defined as early as possible and kept up to date.

The NERC and the Electric Power Research Institute (EPRI) are readily situated to provide much of what is needed to support DHS in carrying out its responsibilities. The Edison Electric Institute, the American Public Power Association, and the North American Rural Electric Cooperative Association are also important components for coordinating activity. Independent power producers and other industry groups normally participate in these groups or have groups of their own. The manufacturers of generation, transmission, and distribution components are another key element of the industry that should be involved. Working closely with industry and these institutions, DHS should provide for the necessary capability to control the system in order to minimize self-destruction in the event of an EMP attack and to recover as rapidly and effectively as possible.

### ***Multiple Benefit***

Most of the recommended initiatives and actions serve multiple purposes and thus are not only to mitigate or protect against an EMP attack and other assaults on the electric power system. The protection of the system and rapid restoration of the system from an EMP attack also are effective against attack from a number of physical threats that directly threaten to destroy or damage key components of the electrical system. Large-scale natural disasters, such as Hurricane Katrina, also are in large part mitigated by these

---



same initiatives. Many of the initiatives enhance reliability, efficiency, and quality of the electrical supply, which is a direct benefit to the electrical consumer and the U.S. economy.

To the greatest extent feasible, solutions for EMP should be designed to be useful solutions to the broad range of security and reliability challenges. For example, black start resources are essential for many threats, purposeful or not, to the power grid. Integrating cyber security and EMP hardness into control systems simultaneously as these systems are routinely upgraded will be much more effective and less costly than doing two separate jobs.

### ***Recommended Initiatives***

The following initiatives must be implemented and verified by DHS and DOE, utilizing industry and other governmental institutions to assure the most cost effective outcome occurs and that it does so more rapidly than otherwise possible. In many instances, these initiatives are extensions or expansions of existing procedures and systems such as those of NERC.

- ◆ *Understand system and network level vulnerabilities, including cascading effects*—To better understand EMP-related system response and recovery issues, conduct in-depth research and development on system vulnerabilities. The objective is to identify cost effective and necessary modifications and additions in order to further achieve the overall system performance. Specifically there should be government-sponsored research and development of components and processes to identify and develop new consequential and cost effective approaches and activities.
- ◆ *Evaluate and implement quick fixes*—Identify what may presently be available commercially to provide cost effective patches and snap-on modifications to quickly provide significant protection and limit damage to high-value generation and transmission assets as well as emergency generation and black start capability. These include installation or modification of equipment as well as changes in operating practices. This is both fast and low cost.
- ◆ *Develop national and regional restoration plans*—The plans must prioritize the rapid restoration of power with an emphasis on restoring critical loads that are identified by the Government. The plans must be combined with the requirements for providing and maintaining emergency power service by these loads. The plans must address outages with wide geographic effect, multiple component failure, poor communication capability, and failure of islanding schemes within the affected area. Government and industry responsibilities must be assigned and clearly delineated. Indemnification arrangements must be put into place to allow industry to implement the Government's priorities as well as deal with potential environmental and electrical hazards to ensure rapid recovery. Planning must address not only the usual contingency for return to normal operating condition, but also restoration to a reduced capability for minimum necessary service. Service priorities under duress may be different from priorities under normal conditions. The planning basis for reduced capability should be the minimum necessary connectivity, generation assumptions based on reduced fuel availability scenarios, and reduced load, with the goal of universal service at limited power. National Guard and other relevant resources and capabilities must be incorporated.
- ◆ *Assure availability of replacement equipment*—On hand or readily available spare parts to repair or replace damaged electronic and larger power system components



must be available in sufficient quantities and in locations to allow for rapid correction and restoration commensurate with a post-EMP attack and its impacts on related infrastructures such as communication and transportation. NERC already has a spare component database for such large items as transformers and breakers that is expanding to include delivery capability, but now must be revised to accommodate an EMP attack environment. Where additional spare components need to be acquired or delivery made possible to critical locations, DHS must work with NERC and industry to identify the need and provide the spares or delivery capability; such as the critical material and strategic petroleum reserves and similar strategic reserves. The key will be to decide where to draw the line between reserves for reliability and those for security. It also will be necessary to keep the equipment current. In addition, strategic manufacturing and repair facilities themselves might be provided with emergency generation to minimize stockpiles. This would also be of benefit to industry as well as enhance security. Research is underway and should be further pursued, into the production of multiple use emergency replacement transformers, breakers, controls, and other critical equipment. Such devices would trade efficiency and device service life for modularity, transportability and affordability. They would not be planned for normal use. Movement, stockpiles and protection of stockpiles must be integrated with National Guard and other relevant capabilities.

- ◆ *Assure availability of critical communications channels*—Assure that throughout the system there are local and system-wide backup EMP survivable communication systems adequate for command and control of operations and restoration of the electrical system. The most critical communications channels are the ones that enable recovery, not normal operations. Planning must presume that, for the near term at least, computer-based control systems will not be capable of supporting post-EMP operations. The most critical communication assets are thus the in-house ones that enable manual operation and system diagnostics. Dispatch communication is next in importance. Communications to coordinate black start are also vital. NERC should review and upgrade operating procedures and information exchanges between and among existing control centers, key substations, and generating plants to recognize and deal as effectively as possible with EMP, building upon the systems, procedures, and databases currently in place. Local emergency and 9-1-1 communications centers, the National Guard and other relevant communication systems, and redundant capabilities should be incorporated where possible.
- ◆ *Expand and extend emergency power supplies*—Add to the number of stand-alone back-up and emergency power supplies such as diesels and long-life batteries. This addition is vital and a least-cost protection of critical service. The loss of emergency power before restoration of the external power supply is likely to occur in present circumstances and is highly probable to be devastating. Presently such emergency power is useable only for relatively short periods due mostly to at-site stored fuel limitations, which have become increasingly limited. The length of time recommended for each location and load will be determined by DHS and industry where the emergency supply is private, such as with hospitals, financial institutions, and telecommunication stations. The specific recommendations are:
  - Increase the battery and on-site generating capability for key substation and control facilities to extend the critical period allowing recovery. This action is relatively low cost and will improve reliability as well as provide substantial protection against all forms of attack.

- Require key gasoline and diesel fuel service stations and liquid fuel distribution facilities in geographic areas to have at-site generation, fueled from existing at-site storage to assure fuel for transportation and other services, including refueling emergency generators in the immediate area.
  - Require that key fueling stations for the railroads have standby generation much as the previously mentioned service stations and distribution facilities.
  - Require the emergency generator start, operation, and interconnection mechanisms to be EMP hardened or manual. This action will also require the ability to isolate these facilities from the main electrical power system during emergency generation operation and require that such isolation switching be EMP hardened.
  - Where within safety parameters extend the emergency generation life through greater fuel storage or supply sources (with their own emergency power supplies). Fuel supplies for more critical facilities must be extended to at least a week or longer, where possible. This action will probably entail careful use or development of relatively near location (but not contiguous) fuel stockpiles with their own emergency generation.
  - Regularly test and verify the emergency operations. If the Government were to enforce current regulations, many of the public facilities with standby generation would be routinely tested and failures could be avoided.
  - Provide for the local integration of railroad mobile diesel electric units with switching and controls hardened against EMP. The same should be provided for large ships at major ports.
- ◆ *Extend black start capability*—Systemwide black start capabilities must be assured and exercised to allow for smaller and better islanding and faster restoration. The installation of substantially more black start generations units and dual feed capable units (e.g., natural gas-fired units that can operate on #2 oil stored on site) coupled with specific transmission that can be readily isolated to balance loads for restoration is necessary. Sufficient fuel must be provided to substantially expand the critical period for recovery such as with multiple start attempts. The NERC regions now do surveys of available black start and fuel switchable generation. Requiring all power plants above a certain significant size to have black start or at-site fuel switching capability (with at-site stored fuel) would be a very small added expense, and would provide major benefits against all disruptions including nonadversarial, so it is both an industry and security benefit. The start, operation, and control systems for such capability have to be EMP hardened or manual, recognizing that most large power plants have personnel on site.
- ◆ *Prioritize and protect critical nodes*— Government entities, such as DHS and DOE, must identify promptly those specific loads that are critical to either remain in service or to be restored as a priority with target restoration to be within a matter of hours following an EMP attack. These may well include loads necessary to assure the continuation of all forms of emergency response care and recovery. These must include what is necessary to avoid collapse of, or allow for the rapid recovery of financial systems, key telecommunication systems, the Government's command and control in the civilian sector, and those elements that allow for rapid and effective recovery of the electric power system in a more general sense. These loads must be prioritized so that the most critical can be protected and designed for rapid restoration in the near term and then add more next-level priority loads as resources permit. The above recommendations for extended and adequate emergency power supply are the most direct

and cost efficient approach. The shift to nonsynchronous, interconnected islands is the secondary application, but it will take longer and is more expensive. Providing such islands of small-to-modest size to support large loads can best assure no loss of power supply or far more rapid restoration.

- ◆ *Expand and assure intelligent islanding capability*—Direct the electrical system institutions and entities to expand the capability of the system to break into islands of matching load and generation, enhancing what now exists to minimize the impact and provide for more rapid and widespread recovery. The establishment of nonsynchronous connections between subregions, perhaps beginning with NERC already identified subregions, should be required. This can readily be accomplished today with approaches such as DC back-to-back converter installations that facilitate power transfers but maintain a barrier. This mode of operation between regions is often referred to as maintaining frequency independence. Reconfiguration of the Eastern Connected System into a number of such nonsynchronous connected regions could eliminate large service interruptions, while still maintaining the present interconnection status. It may be a priority to first establish smaller islands of frequency independence to better assure power supply to government-identified critical loads that are nominally too large for most emergency power supplies, such as large financial centers, and telecommunication hubs. Incidental to any studies could be new ideas for conversion of HVAC transmission lines to HVDC operation for greater transmission capacity as a further and corollary benefit. Also new ideas are being discussed, such as, where the converter transformers can be eliminated, resulting in a substantial cost reduction. Asynchronous regional connections is a common term used to identify this broad area technically. The protective and control systems necessary to implement this capability will have to be hardened. It will not be a retrofit but simply a part of the initial design and procedures, so the cost for EMP protection is small. Note that the DC or other interface making the nonsynchronous connection possible is not sized for the entire electrical capacity within the respective island but is sufficient only for reliability and commercial transactions, which normally is far less. Sizing this interface is a special effort that needs to be established primarily by NERC and FERC but with Federal coordination. Breaking the larger electrical power system into subsystem islands of matching load and generation will enhance what now exists to minimize the impact, decrease likelihood of broad systemwide collapse, and provide for more rapid and widespread recovery. It is just as useful for normal reliability against random disturbances or natural disasters in reducing size and time for blackouts. Thus it is critical for protection and restoration coming from any type of attack, not just EMP. Ensuring this islanding capability in the event of EMP is critical, although it requires a longer-term system design and implementation.

- ◆ *Assure protection of high-value generation assets*—Enhance the survivability of generating plants at the point of system collapse due to the very broad and simultaneous nature of an EMP attack. NERC, EPRI, equipment and control system providers, and utilities need to aggressively evaluate and verify what is vulnerable to EMP and commensurate consequences. Generating plants can be severely damaged from large electrical faults or incursions in the absence of protective devices. They can also be occasionally damaged in the event of sudden load loss if protective shutdown systems fail. Control systems used in generation facilities are inherently less robust than their counterparts in transmission and thus are more susceptible to EMP disruption. They are highly computer controlled which further exacerbates their risk to EMP. Yet at the

same time, they have trained personnel on site who with proper training, procedures, and spare parts, can greatly assist in restoration. System-level protection assurance is more complex due to the need for multiple systems to function in proper sequence. Lead times on generation components are even longer than for major transmission components. Existing coal plants make up nearly half the Nation's generation, but they generally have the most robust control systems with many remaining electro-mechanical controls still in operation. Natural gas-fired combustion turbines and associated steam secondary systems represent the newest significant contribution to the generation. These are mostly all modern electronic- and computer-based control and protective systems and are considered very vulnerable to EMP. Their fuel systems are not on site and will also be interrupted due to EMP. Nuclear plants have many redundant and fail-safe systems, but they too are very electronically controlled. The key difference with nuclear power plants is the extensive manual control capability and training, making them less vulnerable than the others. Hydroelectric is the next substantial generation element and is the most robust, although its older mechanical and electromechanical controls are being replaced at a rapid rate. Black start generation is normally quite secure but start and frequency controls will need to be protected from EMP. The highest priority generation assets are those needed for black start, but all are critical for restoration of any meaningful service.

- ◆ *Assure protection of high-value transmission assets*—Ability to withstand EMP must be assured at the system level. Priority for protection is on the highest voltage, and on the highest power units serving the longest lines; these require the most time to replace and are the most vulnerable in the absence of normal protections due to E1 and provide the major flow and delivery of power. Provisions must be made for the protection of large high-value assets such as transformers and breakers against the loss of protection and sequential subsequent impacts from E2 and E3 creating damage. E3 ground-induced current impacts are important from an industry standpoint since they can occur beyond E3 due to the risk of large, 100-year geomagnetic solar storms. For E3 this could include adding either permanent or switchable resistance to ground in the neutral of large transformers. This protection would then be available upon notice of the onset of a solar storm or sufficient threat of EMP attack. Thus it provides a simple expedient that does not compromise performance under normal operation. Due to the interconnected nature of the grid and to the need for that connectivity to enable recovery, the likelihood of a blackout lasting years over large portions of the affected region is substantial with damage to these high-value components. The islanding of the system through nonsynchronous connections may help reduce the E2 and E3 impacts by shortening the long line coupling in some instances.
- ◆ *Assure sufficient numbers of adequately trained recovery personnel*—Expand levels of manpower and training as they are otherwise limited to only that needed for efficient normal power operation that is highly and increasingly computer aided. Industry and government must work together to enhance recovery capability.
- ◆ *Simulate, train, exercise, and test the recovery plan*—Develop two or three centers for the purpose of simulating EMP and other major system threatening attacks. Develop procedures for addressing the impact of such attacks to identify weaknesses, provide training for personnel and develop EMP response training procedures and coordination of all activities and appropriate agencies and industry. While developing response plans, training and coordination are the primary purpose, identifying vulnerabilities through “red team” exercises is also important for identifying, prioritizing, and recti-



fying weaknesses. The centers would each focus on one of the three main integrated electrical networks — Eastern Grid, Western Grid, and Texas. These centers may be able to effectively utilize facilities such as the TVA bunker and the BPA control center in order to conserve resources and achieve rapid results. DOE facilities and other no longer utilized facilities should also be examined. Develop simulators to train and develop procedures similar to the airline industry. Exercising black start will require indemnification of power providers.

- ◆ *Develop and deploy system test standards and equipment*—Test and evaluate the multitude of system components to ensure that system vulnerability to EMP is identified and mitigation and protection efforts are effective. Device-level standards and test equipment exist for normal power line disturbances (EMC standards), but protection at the system level is the more important goal. System-level improvements such as isolators, line protection, and grounding improvements will be the most practical and least expensive in most cases rather than replacement of individual component devices.
- ◆ *Establish installation standards*—More robust installation standards must be identified and implemented as appropriate — such as short shielded cables, circumferential grounding, arrestors on leads, surge protectors, and similar activities. These should include more robust system standards — such as proximity to protected device, no commercial off-the-shelf (COTS) computers in mission critical roles and similar matters. In some instances, these will qualify as add-ons and replacements during the early period initiatives. The Government should complete the testing and evaluation work that the Commission initiated to set hardening standards for electric power protective systems. Government should provide fiscal assistance to industry in implementing the needed hardening solutions.

### **Cost and Funding of Selected Initiatives**

It must be noted that the very wide variety of components; installation techniques; local system designs; age of components, subsystems, and controls located within buildings or exposed; and so forth all drastically affect the type and expense for implementing the recommended initiatives. Internal DHS and other governmental costs are assumed to be absorbed. A significant portion of the labor to affect the modifications is already in place. Often the modification will be part of a program for repair, replacement and modernization that is continuing regardless of the EMP mitigation program. The addition of non-synchronous connection capability once defined is a contract function coupled with at-site staffing and control system interfaces. All of this effort factors into the cost estimates and results in fairly wide ranges in most instances. Only the costs for some of the larger or more system-specific initiatives are estimated here (in 2007 dollars).

- ◆ There are several thousand major transformers and other high-value components on the transmission grid. Protective relays and sensors for these components are more than that number but less than twice. A continual program of replacement and upgrade with EMP-hardened components will substantially reduce the cost attributable uniquely to EMP. Labor for installation is already a part of the industry work force. The estimated cost for add-on and EMP-hardened replacement units and EMP protection schemes is in the range of \$250 million to \$500 million.
- ◆ Approximately 5,000 generating plants of significance will need some form of added protection against EMP, particularly for their control systems. In some instances the

fix is quite inexpensive and in others it will require major replacements. The estimated cost is in the range of \$100 million to \$250 million.

- ◆ The addition of nonsynchronous interfaces to create subregion islands is not known with reasonable certainty, but it might be in the order of \$100 million to \$150 million per island. The pace of creating islands and their priority will be established by DHS in consultation with NERC and FERC. Moving to at least six or more fairly rapidly is a fair assumption. There will be annual operating costs of around \$5 million per island.
- ◆ The simulation and training centers are assumed at three — one for each interconnect — for a cost in the range of \$100 million to \$250 million plus annual operating costs of around \$25 million per year.
- ◆ Protection of controls for emergency power supplies should not be too expensive since hard-wired manual start and run capability should be in place for many, which is adequate. Furthermore, the test, adjust, and verification will be carried out by the entity that owns the emergency power supply as part of normal operating procedures. Retrofit of protective devices such as filters might be accomplished at a cost of less than \$30,000 per generator for newer generators with vulnerable electronic controls. Hardening the connection to the rest of the facility power system requires a protected internal distribution system from the backup generator.
- ◆ Switchable ground resistors for high-value transformers are estimated to cost in the range of \$75 million to \$150 million.
- ◆ The addition of new black start generation with system integration and protected controls is estimated to cost around \$12 million per installation. Probably no more than 150 such installations will need to be added throughout the United States and Canadian provinces. Adding dual fuel capability to natural gas-fired generation is done for the economic purpose of the owner, yet it has the same value as the addition of black start generation. The addition of fuel storage for the existing black start units is relatively small, about \$1 million each.
- ◆ The addition of emergency generation at the multitude of sites including fuel and transportation sites is probably around \$2 million to \$5 million each.
- ◆ The cost for monitoring, on a continuous basis, the state of the electric infrastructure, its topology, and key elements plus for assessing the actual EMP vulnerability, validation of mitigation and protection, maintenance, and surveillance data for the system at large cannot be estimated since it falls under many existing government-funded activities, but in any event, it is not considered significant.
- ◆ Research and development activities are a level-of-effort funding that needs to be decided by DHS. Redirection of existing funding is also likely to occur.
- ◆ Funding for the initiatives above is to be divided between industry and government. Government is responsible for those activities that relate directly and uniquely to the purpose of assuring continuation of the necessary functioning of U.S. society in the face of an EMP attack or other broadly targeted physical or information systems attack. Industry is responsible for all other activities including reliability, efficiency and commercial interests. Industry is also the best source for advice on cost effective implementation of the initiatives.





## Chapter 3. Telecommunications

### Introduction

Telecommunications provides the connectivity that links the elements of our society together. It is a vital capability that plays an integral role in the normal day-to-day routine of the civilian, business, and government sectors of society. It is a critical enabler for the functioning of our national financial infrastructure, as transactions representing trillions of dollars flow daily via telecommunications. It enables agencies of local, state, and federal government to discharge their duties. People can communicate on the go, almost anytime and virtually anywhere because of telecommunications, as exemplified by more than 100 million cellular subscribers in the United States (U.S.). Telecommunications provides a vital pathway between emergency response personnel in crisis situations. It has transformed, via the Internet and advances in technology, the way business and society in general operate. Downloading music and video content using the Internet instead of in-store purchases, using cell phones to interactively gather travel directions instead of using paper maps, and using remote sensors and video streams to send security information over a communications network to a central site for appropriate dispatch instead of using on-site security guards are examples of these changes.

Telecommunications can be thought of as:

- ◆ The mix of equipment used to initiate and receive voice, data, and video messages (e.g., cell phones and personal computers).
- ◆ The associated media (e.g., fiber optics and copper) and equipment (e.g., multiplexers) that transport those messages.
- ◆ The equipment that routes the messages between destinations (e.g., Internet Protocol [IP]-based routers).
- ◆ The basic and enhanced services offered by communications carriers such as AT&T, Verizon Wireless, and Comcast.
- ◆ The supporting monitoring and management systems that identify, mitigate, and repair problems that can impact performance of services.
- ◆ The supporting administrative systems for functions such as billing.

This chapter discusses civilian telecommunications. Among the main trends to consider in evaluating the impact of EMP on these telecommunications networks in the next 15 years are:

- ◆ The dramatic growth in the number of wireless networks and in the use of wireless services.
- ◆ Improvements in the technology and reliability associated with optical networks leveraging heavy fiber deployment (fiber is generally viewed positively in terms of EMP survivability).
- ◆ Shrinking work forces used in managing networks and an associated increase in dependence on automation and software “diagnostic smarts” to support maintenance, problem isolation and recovery, and other performance impacting functions.
- ◆ An architectural evolution toward a converged network in which voice, data, and video traffic are carried over the same network.

When fully implemented, this evolution to a converged network will represent a major change-out of the equipment that existed in the 1990s, and that still exists, in the U.S.

telecommunications network. Thus, it represents an opportunity for EMP hardening considerations to be included as the transition occurs.

Telecommunications service providers have proclaimed that carrying voice, data, and video together over converged networks is an underpinning of their strategic directions. Service providers point to the fact that traffic residing on embedded, older technology will be transitioned to this new converged network within financial and regulatory constraints.<sup>1</sup> While this converged network evolution has begun, it is expected to continue for an additional decade or more.

The reason for a lengthy transition can be better understood by reviewing some historical factors related to the U.S. telecommunications network. Several factors led to traffic being carried by separate networks, including differences in the characteristics of voice, data, and video traffic; the relative dominance in the amount of voice traffic over data and video; and the technological state of the carrier network equipment.

With respect to traffic characteristics:

- ◆ Voice communications generally are characterized by real-time interactions with typical durations of a few minutes.
- ◆ Data communications tend to occur in bursts and may consume large amounts of bandwidth during these bursts. Data communications users often access networks for long holding times that may range into hours.
- ◆ Video traffic typically is characterized by high-bandwidth, long-duration, one-way transmission such as distributing cable TV content to viewers with lower-bandwidth traffic sent from the subscriber to the service provider, for example, to signal the selection of a specific on-demand program.

With respect to traffic mixes:

- ◆ As the 1990s progressed, the growth of data traffic exploded, fueled in large part by Internet usage. Data communications growth is continuing at a rapid pace, while growth in voice has remained relatively flat. Some estimates have data traffic already exceeding voice traffic beginning around the year 2000.
- ◆ The growth in data communications traffic has made it more fiscally attractive to find technological solutions that avoid the expense of maintaining separate voice and data networks.

With respect to technology evolution:

- ◆ Voice communications over the past decade have been handled primarily by carrier equipment called digital circuit switches. The switches are engineered based on statistical usage of the network that assumes not all of the individual users, traditionally in the thousands, served by those individual switches will try to gain access simultaneously. These switches, of which several thousand are deployed, were not designed to effectively handle the characteristics of data and video traffic.
- ◆ Router technology has evolved rapidly. Advances in protocols that support assigning quality of service (QoS) requirements for different traffic mixes and greater processing speed and capacity have provided solutions for handling voice, data, and video using a common set of equipment.

---

<sup>1</sup> Wegleitner, Mark, Verizon, Senior Vice President, Broadband Packet Evolution, Technology, 2005.

- ◆ Service providers implement new technologies slowly. This is prudent given the complexity of the networks in question and a desire to prove-in technologies and fine-tune network management procedures prior to wide-scale deployment.

### Telecommunications Support During Emergencies

There is a recognition at the highest levels of government and industry that telecommunications plays a critical role, not only in the normal day-to-day operations of society, but also in reconstituting societal functions and mitigating human, financial, and physical infrastructure losses during man-made and natural disasters. This has led to government and industry partnering to codify processes, organizational structures, and services to address these disasters. Among these codifications are the National Communications System (NCS) and a set of services known as National Security and Emergency Preparedness (NS/EP) services.

The NCS was established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*.<sup>2</sup> These functions include administering the National Coordinating Center for Telecommunications (NCC) to facilitate the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities under all crises and emergencies; developing and ensuring the implementation of plans and programs that support the viability of telecommunications infrastructure hardness, redundancy, mobility, connectivity, and security; and serving as the focal point for joint industry-government and interagency NS/EP telecommunications planning and partnerships.

With respect to the NS/EP telecommunications services, a set of evolving capabilities exist for:

- ◆ Prioritizing telephone calls through the wireline and wireless networks during time intervals when call volumes are excessive and facilities may be degraded.
- ◆ Giving priority to restoring emergency and essential services that may be damaged or degraded.
- ◆ Rapidly getting new telecommunications connections into operation.
- ◆ Keeping carriers communicating with government and one another on an on-going basis during crises events.

NS/EP-related definitions are noted below.

NS/EP Definitions
<i>NS/EP Telecommunications Services</i> —Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States. ( <i>Telecommunications Service Priority [TSP] System for National Security Emergency Preparedness: Service User Manual, NCS Manual 3-1-1, Appendix A, July 9, 1990</i> )
<i>NS/EP Requirements</i> —Features that maintain a state of readiness or respond to and manage an event or crisis (local, national, or international), which causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the NS/EP posture of the United States. (Federal Standard 1037C)
<i>Emergency NS/EP and Essential NS/EP</i> —Emergency NS/EP telecommunication services are those new services that are “so critical as to be required to be provisioned at the earliest possible time without regard to the costs of obtaining them.” An example of Emergency NS/EP service is federal government activity in response to a Presidential declared disaster or emergency. Telecommunications services are designated as essential where a disruption of “a few minutes to one day” could seriously affect the continued operations that support the NS/EP function. (Federal Register/Vol. 67, No. 236, December 9, 2002/Notices)

<sup>2</sup> Executive Order 12472, April 3, 1984.

These NCS and NS/EP services are capabilities that would be drawn upon in an EMP event, and they will evolve as the U.S. telecommunications network evolves. This commitment to evolution has been reinforced, for example, by testimony from Frank Libutti (Undersecretary, Information Analysis and Infrastructure Protection, Department of Homeland Security) before the United States Senate Committee on Appropriations in 2004:

The NCS is continuing a diverse set of mature and evolving programs designed to ensure priority use of telecommunications services by NS/EP users during times of national crisis. The more mature services—including the Government Emergency Telecommunications Service (GETS) and the Telecommunications Service Priority (TSP)—were instrumental in the response to the September 11 attacks. FY 2005 funding enhances these programs and supports added development of the Wireless Priority Service (WPS) program and upgrades to the Special Routing Arrangement Service (SRAS). Specifically, priority service programs include: (1) GETS, which offers nationwide priority voice and low-speed data service during an emergency or crisis situation; (2) WPS, which provides a nationwide priority cellular service to key NS/EP users, including individuals from Federal, state and local governments and the private sector; (3) TSP, which provides the administrative and operational framework for priority provisioning and restoration of critical NS/EP telecommunications services. In place since the mid-1980s, more than 50,000 circuits are protected today under TSP, including circuits associated with critical infrastructures such as electric power, telecommunications, and financial services.; (4) SRAS, which is a variant of GETS to support the Continuity of Government (COG) program including the reengineering of SRAS in the AT&T network and development of SRAS capabilities in the MCI and Sprint networks, and; (5) the Alerting and Coordination Network (ACN) which is an NCS program that provides dedicated communications between selected critical government and telecommunications industry operations centers.<sup>3</sup>

### EMP Impact on Telecommunications

To aid in understanding the impact of EMP on telecommunications, **figure 3-1** provides a simplified diagram of a telecommunications network.

Service subscribers communicate through a local node. For example, a cellular subscriber communicates through a cell tower controlled by a cellular base station. If communication is with a party located on another local node, the communications traffic may be routed through the backbone to the distant local node for delivery to the other party. The backbone connects to thousands of local nodes and in doing so serves a transport and routing function to move voice, data, or video traffic between or among the communicators. It consists of a mix of equipment that provides high-speed connectivity between the local nodes. In an actual network if there is sufficient traffic between two local nodes, they may be directly connected by transmission media such as fiber links. **Figure 3-1** shows some network equipment, such as a digital switch and a network router. The control network collects information statistics from the equipment in the local nodes and

---

<sup>3</sup> [http://www.globalsecurity.org/security/library/congress/2004\\_h/040302-libutti.htm](http://www.globalsecurity.org/security/library/congress/2004_h/040302-libutti.htm).

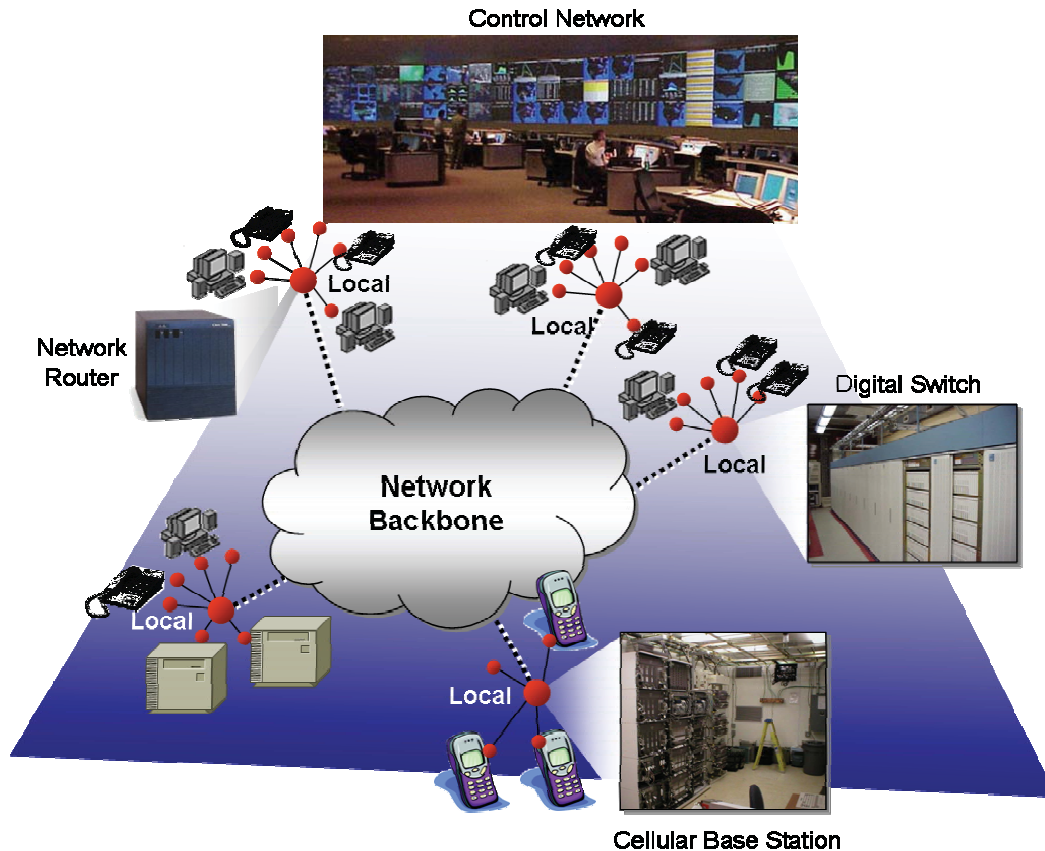


Figure 3-1. Generic Telecommunications Network Architecture

backbone that help manage the network's performance. The backbone has been the main focus of industry in deploying components of the converged network to date, and it is the furthest along with respect to the converged network vision.

A set of first-order assumptions drove the analytical assessment of EMP impacts on telecommunications:

- ◆ In a crisis, voice services will be viewed as critical, with the percent of call attempts completed as a key metric.
- ◆ The backbone, as depicted in **figure 3-1**, is where the greatest influx of new equipment has been deployed. This is newer-vintage, expensive, high-end routing and transport equipment connected by fiber optics. An assumption is that the equipment will be highly survivable up to high E1 EMP levels and perhaps will experience only transient effects at those levels, but this needs to be verified with further testing.
- ◆ The local nodes will be replaced with equipment supporting the converged network vision, but this change-out will continue beyond the time frame examined in this Commission study. Commission-sponsored testing provided insights into the performance of the new equipment that is being incorporated into the converged network. Among the current local node equipment are digital circuit switches and other equipment that have been tested and analyzed as part of a prior assessment of E1 EMP on telecommunications conducted in the early 1990s.<sup>4</sup> In this study, circuit switch

<sup>4</sup> For example, Network Level EMP Effects Evaluation of the Primary PSN Toll-Level Networks, Office of the Manager: NCS, January 1994.



manufacturers noted they would be incorporating equipment changes to address a majority of the items shown to be susceptible to E1 EMP in the products tested, and the Commission assessments assume this to be the case.

Keeping these factors in mind, the Commission focused its analytical efforts on customer premises equipment (CPE), the subsequent impact on demand levels at the local nodes and local node equipment, and the subsequent ability to complete calls assuming a robust backbone.

On the demand side, call origination electronic assets have the potential for EMP disruption or damage. A key issue is whether EMP will impact the operation of telephones, cell phones, and computer systems (like those shown in **figure 3-1**) and, as such, reduce the demand placed on assets in the local and backbone elements that move information between information senders and receivers.

The major elements of the civilian telecommunication network are electronic systems with circuit boards, integrated circuit chips, and cable connections such as routers that switch and transport information between users of the network (e.g., transport phone calls). Like the equipment that generates demand on the network, these electronics have an inherent vulnerability to EMP threats. The majority of these critical switching and transport assets that are part of the local and backbone nodes in **figure 3-1** are housed in Central Offices (COs). Typically COs are windowless concrete buildings. Sometimes equipment used to provide service to end users is housed in Controlled Environmental Vaults (CEV). These are smaller structures that provide environmental control similar to that of a CO. Wireless base stations supporting cellular communications are housed in structures similar to CEVs. Finally, some equipment such as that used to provide high-speed Internet service may be installed in small cabinets and enclosures without environmental controls.

Regardless of the installation location, telecommunications equipment and the facilities that contain them follow strict rules and requirements to protect against natural or unintentional electromagnetic disturbances, such as lightning, electromagnetic interference, electrostatic discharge, and power influences on telecom cables. Typical protection techniques include grounding, bonding, shielding, and the use of surge protective devices. However, an EMP attack exhibits unique characteristics, such as rapid rise-time transients, and the existing protection measures were not specifically intended for or tested against EMP.

Given these network characteristics, some factors that contribute to mitigating EMP effects on telecommunications are:

- ◆ Industrywide groups that systematically share best practices and lessons learned to improve network reliability, such as the Network Reliability and Interoperability Council (NRIC).
- ◆ Availability of NS/EP telecommunications capabilities.
- ◆ Volume, geographic diversity, and redundant deployment of telecommunications equipment assets, coupled with wireline, wireless, satellite, and radio as alternative means for communications.
- ◆ Deployment of fiber-optic technology within telecommunications carrier networks.
- ◆ Use of standard bonding and grounding practices for telecommunications equipment deployed in carrier networks.

- ◆ Historical performance of terrestrial carrier networks in electromagnetic events such as lightning and geomagnetic storms.

The Commission sponsored testing and analytical efforts that led to the conclusion that an EMP attack would disrupt or damage a functionally significant fraction of the electronic circuits in the Nation's civilian telecommunications systems in the geographic region exposed to EMP. Cellular networks are seen as being less robust to EMP than landline networks due to a combination of the higher susceptibility of cellular network equipment to damage and more limited backup power capacity at cell sites than at counterpart landline network equipment sites.

The analysis suggested that damage to telephones, cell phones, and other communications devices would not be sufficient to curtail higher than normal call volumes on the civilian telecommunications network after exposure to either low or high E1 EMP levels. As such, the remaining operational network would be subjected to high levels of call attempts for some period of time after the attack, leading to degraded telecommunications services. Key government and nongovernment personnel will need priority access to use public network resources to coordinate and support local, regional, and national recovery efforts. This will be especially problematic during the interval of severe network congestion. Services such as GETS will be crucially important during these periods of high call demand.

The Commission's expectation is that the impact of a low E1 EMP level exposure would be dominated by the inability to handle the spike in call traffic on landline networks, because the direct impacts on equipment are expected to be largely transient and short term in nature (minutes to hours) with minimal manual restoration. For cellular networks, the impact will be greater (minutes to days) due to the expected levels of manual recovery, more limited backup power at cell sites, and the large number of cellular base stations that serve as key controllers of communications between cell towers and cell phones. The results of limited testing on cellular base stations indicate EMP vulnerabilities that require further examination.

As noted in the electric power section of the Commission report, the loss of portions of the power grid is likely, even for a relatively low-level EMP attack. The longer-term performance of the public telecommunications network and associated NS/EP services will depend, therefore, on the use of backup power capabilities and the rapidity with which primary power can be restored. To offset a loss of electric power, telecommunication sites now use a mix of batteries, mobile generators, and fixed-location generators. Typically, these have 4 to 72 hours of backup power available on-site and thus will depend on either the resumption of electrical utility power or fuel deliveries to function for longer periods of time. A short-term electric power grid outage (less than a few days) would not cause a significant loss of telecom services due to the existence of power backup systems and best practices supporting these critical systems.

In the case of high amplitude E1 EMP level exposures, spikes in call traffic, coupled with a mix of transient impacts and damage requiring manual network equipment restoration, will result in degraded landline and cellular communications on the order of days to weeks. As in the case of low E1 levels, longer-term impacts from power outages could extend the period and severity of the degradation.

General results from the Commission's EMP analysis received concurrence from the NCS as noted below.

**Senate Testimony (March 2005)**

In March 2005 testimony before a U.S. Senate subcommittee (Terrorism and the EMP Threat to Homeland Security, Subcommittee on Terrorism, Technology, and Homeland Security, March 8, 2005), the Acting Director of the NCS noted that “Just last year, the NCS also actively participated in the congressionally-chartered *Commission to Assess the Threat from High Altitude Electromagnetic Pulse* (the 2004 EMP Commission) that examined and evaluated the state of the EMP threat at present and looking 15 years into the foreseeable future. The Commission’s Report, delivered last July, concludes that EMP presents a less significant direct threat to telecommunications than it does to the National Power grid but would nevertheless disrupt or damage a functionally significant fraction of the electronic circuits in the Nation’s telecommunications systems in the region exposed to EMP (which could include most of the United States). The NCS concurs with this assessment.”

**Analysis Approach**

To estimate the impact of an EMP attack on the civilian telecommunications network, the following major tasks were performed:

- ◆ Reviewed lessons learned with respect to telecommunications critical dependencies and susceptibilities from past studies of events, such as major disasters and Year 2000 (Y2K).
- ◆ Visited telecommunications facilities to get “ground truth” insights into possible areas of EMP susceptibility and for data such as equipment layouts to support illustrative testing of telecommunications equipment.
- ◆ Reviewed past test data and performed illustrative testing of wireline and cellular communications devices such as cell phones and network equipment such as network routers to determine EMP susceptibilities.
- ◆ Developed models of telephone network restoration processes and network call processing associated with alternative EMP scenarios using subject matter expert judgment, illustrative test data, and augmentation of existing models to estimate degradation levels for networks. Network statistics such as call completion levels used to estimate degradation were generated for users, assuming they were not using NS/EP services such as GETS.

**Analysis Approach—Lessons Learned**

From interviews and reviews of lessons learned from past outage events, the following issues were identified that helped shape Commission recommendations and provided input for the testing and modeling activities:

- ◆ Y2K contingency planning and past outage events, such as the Hurricane Katrina blackout, point to the need for a functioning voice communications network in an emergency situation to support restoration efforts for multiple critical infrastructures. For example, with respect to managing the power grid, reference material associated with Y2K preparations noted, “The principal strategy is to operate using a manual transfer of a minimum set of critical information ... electric systems must provide sufficient redundancy to assure voice communications over a geographic area that addresses its critical facilities and interfaces to neighboring systems and regional centers.”<sup>5</sup>
- ◆ Conditions that would lead to multi-day unavailability of power remain a principal concern of telecommunications providers. Extended power outages will exacerbate attempts to repair damage and lead to fuel shortages that end up taking network capacity off-line. This concern was reinforced by Hurricane Katrina and by the August

<sup>5</sup> <http://www.y2k.gov/docs/infrastructure.htm>.

2003 Northeast Power Outage. The latter was a key topic of the August 27, 2003, NRIC meeting.

- ◆ A high level of call attempts on both wireline and wireless networks will follow an EMP attack, thereby reducing the effectiveness of voice communications for some time period. At least four times the normal call traffic will likely be experienced by these networks. In previous disasters, these high levels generally lasted for 4 to 8 hours and remained slightly elevated for the first 12 to 24 hours after the event. The spike in call volumes results in callers experiencing problems in successful call completion. Additionally, callers may experience conditions such as delayed dial tones or “all circuits busy” announcements. As an example, the high blocking levels experienced by callers on cellular networks on September 11, 2001, in Washington, D.C., and New York City are shown in **figure 3-2** as call attempts rose to levels as high as 12 times normal.<sup>6</sup>

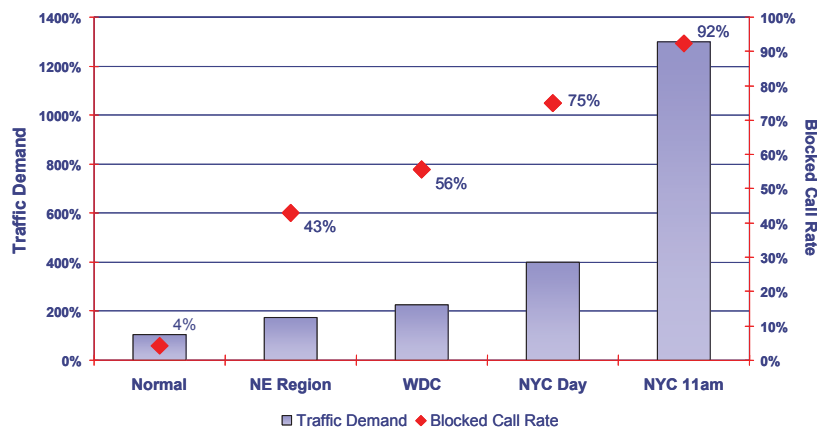


Figure 3-2. September 11, 2001, Blocked Call Rate—Cellular Networks

- ◆ As previously noted, concerns over the ability of key personnel to get calls through the public telecommunications network in a disaster was one of the catalysts for services development that occurred under the leadership of the NCS. GETS and WPS are services intended for use in emergency conditions to improve the probability of key personnel completing calls even when wireline and wireless network are under extremely heavy call loads. These services will be leveraged during an EMP event, but their benefits for subscribers are mitigated when local equipment requires manual recovery to be functional. Based on test results, this manual recovery requirement for cellular base stations is of particular concern.
- ◆ Maintenance and control functions will be critical to restoration and recovery efforts, as they are used by telecommunications carriers to alleviate the overload conditions and identify areas of damage within the network to hasten recovery efforts. For the general populace without access to NS/EP services, if massive call attempts tie up network resources there would be minimal circuits available to dial out and potentially reduced capability to reach 9-1-1 services. To help alleviate this, personnel in a Network Management Center (see **figure 3-3**) could issue a command to the carrier network for “call gapping” through a few quick keystrokes on a personal computer. Through this command, some percentage of calls would be stopped at the originating

<sup>6</sup> Aduskevicz, P., J. Condello, Capt. K. Burton, Review of Power Blackout on Telecom, NRIC, August 27, 2003, quarterly meeting.

switch and thus free up resources that would be needed for dialing out. Testing conducted as part of the previously referenced NCS-sponsored assessment indicated that some physical damage to circuit switch components linking to these network management facilities would occur, even at very low transient levels. This damage would reduce the ability of recovery efforts to bring systems up to full capacity and affect the ability to remotely implement procedures to address EMP-induced network problems.

#### *Analysis Approach—Collecting Ground Truth*

Prior to conducting testing on equipment, visits were made to carrier facilities to verify some of the assumptions regarding equipment layouts that were used in the test configurations. Sites containing wireline network switching and transport equipment, cellular network switching and transport equipment, and Network Management Center equipment were visited. Features such as cable lengths and bonding and grounding practices and issues such as policies for stockpiling spares were explored during these visits. In addition, discussions were held with personnel involved in telecommunications equipment installation activities, technical requirements development for electromagnetic effects protection, and network monitoring and control activities to vet assumptions made in the equipment testing and modeling activities. **Figure 3-4** shows cellular network base station equipment photographed during one of the visits.

**Figure 3-5** is a photo of router equipment used to collect performance information from carrier equipment and transmit it to a Network Management Center, such as the one in **figure 3-3**.

Based on the collected data, a process for network restoration was developed considering the wide mix of assets that could be affected in an EMP event. The restoration process was reviewed with experts who had been involved in large restoration efforts, including personnel charged with developing software systems to expedite network recovery. These reviews helped augment the restoration process model. This process was used in developing recovery timelines generated in the modeling and simulation activity.

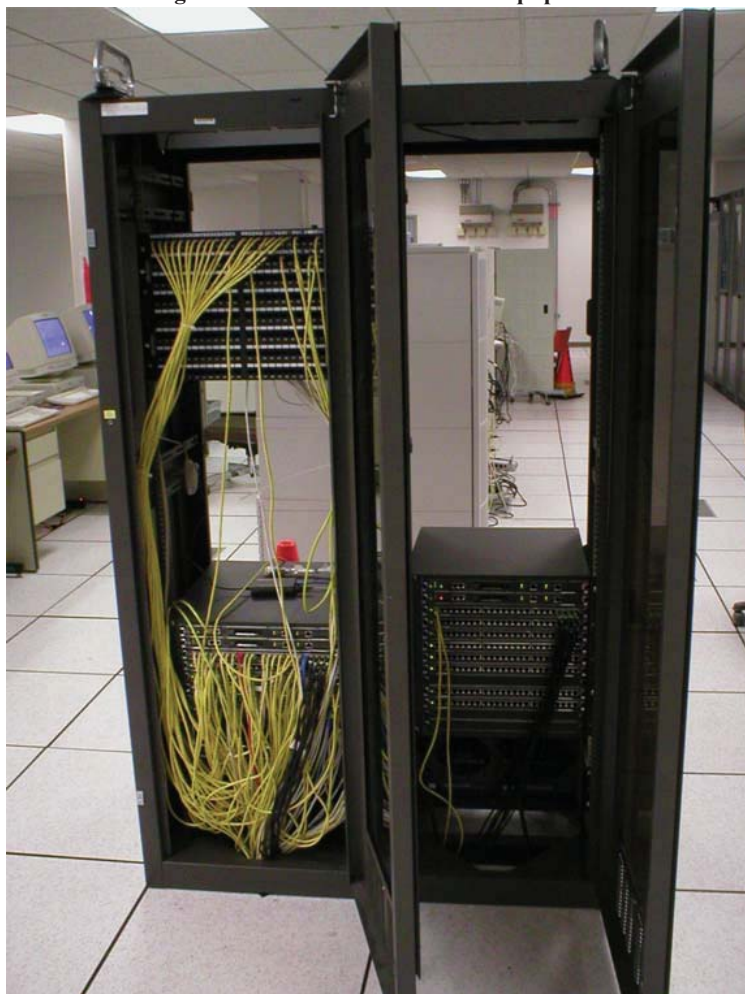


**Figure 3-3. Example Network Management Facility**





**Figure 3-4. Cellular Base Station Equipment**



**Figure 3-5. Routers Collecting Network Management Data**



### *Analysis Approach—Testing for EMP Effects on Telecommunications Networks*

Using the lessons learned and ground truth data described previously, a test plan was developed that focused most heavily on the effects of EMP on voice communications and the associated maintenance and control networks that would support recovery and restoration efforts. Consistent with this, testing activities focused on communications devices and switching and routing equipment expected to play a critical role in supporting future voice communications and on computing equipment supporting the collection of data used for network traffic management. E1 was considered as the primary source of EMP effects on carrier equipment under the assumption that long transport lines within carrier telecommunications networks have moved to fiber instead of copper. We also recognized the growing use of fiber within close proximity to home and business establishments. In accordance with these assumptions, the communications carrier network equipment testing focused on assets that would be considered part of the local nodes in **figure 3-1**.

Prior test data on digital switches, routers, computers, and related equipment were reviewed. For example, during the 1980s and early 1990s, the NCS sponsored testing on major telecommunications switches and transport equipment. The test effort conducted on behalf of the EMP Commission was designed to complement the data available in previously discussed NCS technical reports and other data sources. The test data provided information on the behavior of particular pieces of equipment and was subsequently used to model the impact of an EMP attack on the telecommunications network infrastructure and the recovery process. In addition to network equipment, CPE such as basic telephones and cell phones were tested, as the level of traffic on the public telecommunications networks would be affected by the CPE's EMP survivability. **Table 3-1** lists the telecommunications assets tested at multiple government and commercial facilities, including a rationale for why they were selected. A mixture of continuous wave immersion (CWI), pulse current injection (PCI), and free field illumination tests was used. **Figure 3-6** depicts testing that was conducted at a cellular base station at Idaho National Laboratory (INL). Free-field illumination testing was conducted on equipment covering each of the areas in **table 3-1** (except for cellular network carrier switching equipment [see **figure 3-6**]). The equipment tested included a softswitch, cordless phones, cellular phones, computing servers, Ethernet switches, and routers.

During the testing, in cases where impacts were observed, some were transient in nature, for example, auto-rebooting of softswitch equipment, while some testing resulted in permanent equipment damage and required manual recovery via replacement of components (for example Ethernet card replacement) to address performance degradation.

**Table 3-1. Telecommunications Equipment Tested**

Items	Importance
Corded Phones, Cordless Phones, Cell Phones	Key devices used for voice communications. The level of demand placed on the public telecommunications network will be impacted by the equipments' operational state.
Computing Servers, Secure Access Devices	These computers house software supporting key management and control functions (Network Fault and Traffic Management) critical to network recovery efforts. Since these systems may have to be accessed remotely in an emergency, secure access devices that generate passwords are used to gain access to them.
Routers, Ethernet Switches	Critical equipment supporting the routing of network control and status information between network elements and the facilities and computer systems responsible for their management.

**Table 3-1. Telecommunications Equipment Tested (continued)**

Items	Importance
Softswitches, Gateways	Key equipment being integrated into public networks to support the transmission of voice, data, and video over IP-based technology. This equipment is replacing the digital circuit switches that are part of the local nodes shown in <b>figure 3-1</b> .
Mobile Switching Centers, Base Stations, Base Station Controllers	Major operational components of cellular networks that are used to transmit cellular calls.
Cable Modem Termination System (CMTS), Cable Modems	Cable companies are moving aggressively into telecom, and cable modems are heavily used by customers to access the cable network for communications. The CMTS converts the data signals from cable modems to an Internet Protocol. Trends point to the increased use of routers, Ethernet switches, softswitches, and gateways to route communications traffic.

**Figure 3-6. Cellular Network Testing at INL****Figure 3-7. Testing at NOTES Facility**

**Figure 3-8** shows examples of some of the smaller items tested at the NOTES facility.



Figure 3-8. Secure Access Card and Cell Phones

*Analysis Approach—Modeling and Simulation of EMP Effects*

To develop a view of the system effects that would be caused by an EMP attack, a systematic approach was used in the modeling and simulation effort. The analysis leveraged the Commission-sponsored testing just described, as well as prior equipment testing results. Initially, a telecommunications network performance modeling approach for generating call completion levels given degradation assumptions in wireline and wireless networks was developed for the continental United States. The major assumption in this modeling was that the key area of degradation would be local nodes in the carrier networks (for both wireline and cellular networks). As shown in **figure 3-1**, local nodes are equipment such as the digital circuit switches and cellular base station equipment that provide callers with entry into these wireline and cellular telecommunications networks. Impacts on local nodes could inhibit local calls, as well as prohibit connections to the backbone network that provides for more geographically dispersed communications. Positive trends in the direction of EMP survivability for backbone communications are due to increased routing diversity coupled with heavy fiber deployment, suggesting that a local focus is reasonable in terms of first-order effects.

Following this logic, the modeling steps included:

1. Generate a case study using weapons detonation scenarios that produce electromagnetic field levels modeled over selected geographic regions of the United States and model the impact on network performance (e.g., call completion levels) given the degree of network upset expected to be caused initially by the EMP event. We included transient or self-correcting effects and effects that require human action to correct. The model incorporated past test results from NCS studies and new testing of the equipment listed in **table 3-1**, using assumptions about the types and configurations of equipment that would be deployed in affected areas. The starting point for equipment types was industry databases identifying equipment deployed in telecommunications networks. This was augmented with subject matter expert discussions.
2. Apply generic methods and procedures incorporated in the network restoration process noted earlier to generate recovery times for network equipment. Inputs include engineering assumptions on equipment damage levels, availability of repair personnel, availability of network management and control functions, availability of electric power, and other factors.

3. Use the recovery times to model placing equipment back in service and iteratively estimate network performance levels over time using the network performance model.

The following are illustrative results generated from among scenarios of interest identified by the Commission. **Figures 3-9 through 3-11** show originating call completion levels in the eastern United States for the average combined wireline and wireless calls after an EMP event. Time period categories in these figures include immediately following, 4 hours after, and 48 hours after the EMP event. The results displayed incorporate longer restoration times for cellular equipment, driven in part by levels of manual recovery. **Figure 3-12** shows the recovery curve during the 10-day period following the attack. This is the estimated time period to regain pre-event performance, absent other infrastructure interdependency impacts such as long-term power outages. The shaded circles indicate EMP field-level isocontours generated by the weapon. For example, in **figure 3-9**, the geographic area most negatively impacted has estimated call completion levels of roughly only 4 percent, while the area outside the range of the direct effects has a 73 percent call completion level estimate.

The reason for the 73 percent level is that callers outside the directly affected areas are unable to make calls into the affected areas due to equipment disruptions in those areas, coupled with network congestion and high call-retry levels.

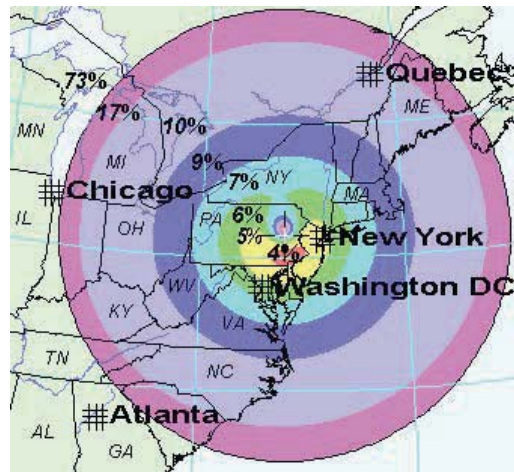


Figure 3-9. Percentage of Calls Completed Immediately After EMP Event

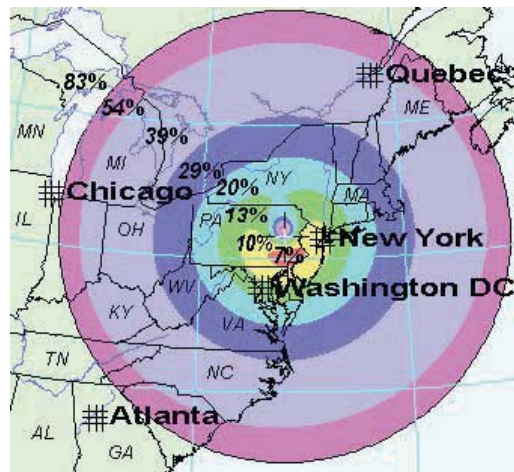


Figure 3-10. Percentage of Calls Completed 4 Hours After EMP Event



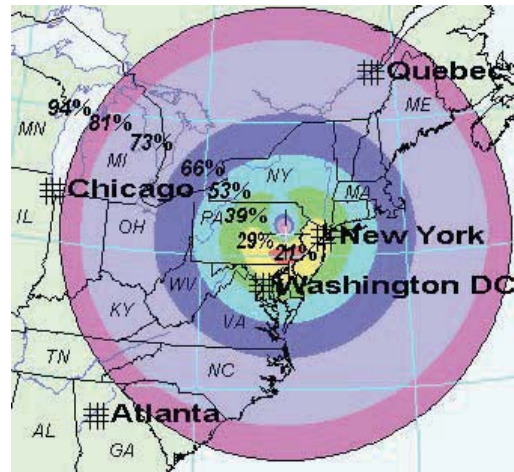


Figure 3-11. Percentage of Calls Completed 2 Days After EMP Event

The illustrative results in **figure 3-12** highlight the value of operational GETS and WPS capabilities given that the call completion levels noted in **figure 3-12** would be unacceptable for NS/EP functions during the critical early stages of an emergency. The analysis performed as part of this EMP Commission effort did not explicitly examine the performance of these NS/EP services in an EMP attack. The call completion levels in **figure 3-12** would be seen as likely lower bounds for these services for the scenarios of interest examined.

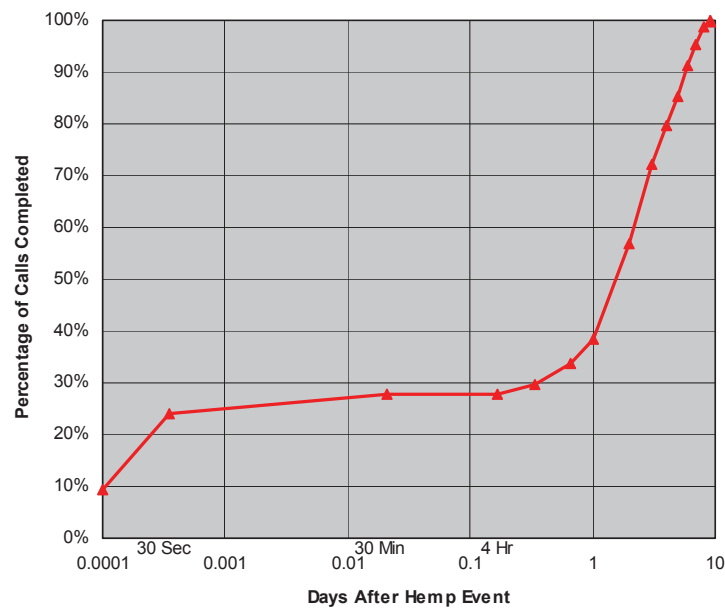


Figure 3-12. Percentage of Calls Completed at Time T  
(Logarithmic Time Scale)  
(Within EMP Contours)

The scenarios examined indicated that even in the case of minimal equipment damage, the functioning of NS/EP telecommunications services are critical to handling the spike in caller traffic expected to follow an EMP attack. This traffic tends to overwhelm the available telecom network capacity and results in degraded network performance. While operational experience exists with the current technologies that support NS/EP services, there is the need to make sure that NS/EP services operate effectively as new technolo-

gies, such as softswitches, are being introduced into the network. It is important to verify that this equipment will operate through an EMP attack under the stressful operating conditions that are anticipated in an emergency situation. The use of IP-related technology such as softswitches to support GETS and WPS services is at the initial point of deployment in local offices. Rigorous analysis is warranted prior to their major deployment to examine EMP survivability issues.

During sensitivity analysis, in the process of examining alternative cellular base station damage levels, an area of concern was identified within the cellular network system. Specifically, the area of concern was degradation of network performance due to EMP effects on critical databases, including the Home Location Registers (HLRs). HLRs contain key user information associated with cellular subscribers, such as account status and location. Within the wireless industry, the deployment approach to achieve HLR diversity (physical and geographic) is mixed. HLRs were not tested for susceptibility levels as part of the EMP Commission study, but using proxy numbers based on testing for circuit switching equipment, sensitivity studies show that it is possible to lose major calling areas in an EMP attack due to HLR degradation. In addition to EMP susceptibility testing, engineering polices and selective EMP hardening of these elements are options that should be examined in the future.

As noted in the Electric Power chapter, loss of portions of the power grid is likely, even for a relatively low-level EMP attack. Our analysis indicates that, in a relatively low-level EMP attack, the direct impact on public telecommunications networks is likely to be dominated by the inability to handle ensuing spikes in call traffic. In such cases, the direct effects on equipment are expected to be largely transient and short term in nature (minutes to hours) with minimal manual restoration needed. However, should widespread loss of primary power occur, the survivability of the telecommunications network and associated NS/EP and other services will depend on the use of backup power capabilities and the rapidity with which primary power can be restored. Most public telecommunications equipment has a mix of battery, mobile generator, and fixed generator support if primary electric power is lost. A short-term loss of the electric power supporting most telecommunications networks today would not cause a major loss of telecom services. This is due to the existence of power backup systems and best practices supporting these critical systems that could sustain telecom services during short-term power outages.

The situation becomes more serious if the power outages are long term and widespread. In such cases, the likely loss of major telecommunications facilities would significantly reduce NS/EP services. A majority of residential telephones today depend on power from local central offices, which would be lost once the backup power at those offices is depleted. Other residential telephones also require commercial power to function. Thus, citizen ability to access 9-1-1 call centers would be a major concern in an extended power outage situation.

Hurricane Katrina in August 2005 damaged cell phone towers and radio antennas. The prolonged blackout resulting from Katrina exhausted the fuel supplies of backup generators servicing emergency communications. Consequently, emergency communications for police, emergency services, and rescue efforts failed. Significantly, these same nodes so critical to emergency communications—cell phone towers and radio antennas—are vulnerable to EMP attack. A protracted blackout resulting from an EMP attack would also exhaust fuel supplies for emergency generators, just as occurred during Hurricane Katrina.

---



Public telecommunications networks can successfully handle a local power outage or short-term outage, such as the August 14, 2003, Northeast blackout. However, a major concern exists with outage durations that range in weeks or months. The widespread collapse of the electric grid due to an EMP event would lead to cascading effects on interdependent infrastructures, as happened during the Katrina blackout. This may well lead to a long-term loss of telecommunications in extended geographic areas outside the power loss. This loss would cascade to any critical applications that depend on telecommunications. As such, telecommunications resilience would greatly benefit from steps to increase power grid and backup power reliability and availability time frames.

Telecommunications network managers have indicated that a key asset in any outage event is the ability to monitor the health of the network in real time to enable rapid response to identified problems. Given the increased level of automation in telecommunications networks coupled with reduction in personnel, it is critical that the telecommunications operations and control functions remain operational in an EMP event. In recovering from an EMP attack, telecommunications carriers will depend on hardware and software systems that help isolate problem areas and implement commands to initiate remediation efforts. Computer servers, personal computers, routers, and related equipment are key components that are housed in Network Management Centers. Carriers typically deploy the equipment in geographically diverse centers in which one center can back up the others. Effects to those centers are moderated in cases in which the centers are separated by distances larger than the EMP footprint.

### **Recommendations**

Based on the analytical efforts performed by this Commission, the following steps are recommended to improve telecommunications performance during and after an EMP event:

- ◆ Successfully evolve critical NS/EP telecommunications services to incorporate the new technologies being embedded into telecommunications networks.
- ◆ Improve the ability of telecommunications services to function for extended periods without the availability of primary power.
- ◆ Adequately address infrastructure interdependency impacts in contingency planning.
- ◆ Identify critical applications that must survive an EMP event and address any shortfalls in telecommunications services that support these applications.

These recommendations are discussed in more detail in the next few sections.

### ***Preventing Widespread Outages from New Technology***

EMP is just one of the potential sources that would lead to stressing telecommunications networks. Understanding NS/EP service performance with respect to IP technology has benefits beyond application to EMP. This issue is in line with a U.S. government interagency Convergence Working Group (CWG) finding<sup>7</sup> that noted, “The FCC should task NRIC to assess the adequacy of interoperability testing between circuit and packet switch networks ... minimize the risk of feature interactions and the introduction of additional vulnerabilities affecting reliability, availability, and security of telecommunication services supporting NS/EP users.”

---

<sup>7</sup> Convergence Working Group’s final report, *Impact of Network Convergence on NS/EP Telecommunications: Findings and Recommendations*, February 2002.

High-profile network failures have occurred as new technologies were introduced into networks. Inadequate testing prior to widespread deployment has been highlighted as a major problem in lessons learned from past outages related to new technology introduction.<sup>8</sup> These offer an incentive for the testing of new technology supporting NS/EP services prior to widespread deployment of the technologies. The use of packet switching technology to support voice services such as GETS and WPS is at the initial point of deployment. Rigorous testing is warranted prior to major deployment. With early identification, specific system EMP vulnerabilities can be addressed prior to widespread deployment.

The following are specific steps to address technology introduction concerns:

- ◆ NCS<sup>9</sup> represents a logical organization to address these areas given its mission associated with the development and maintenance of NS/EP services. NCS should partner with other appropriate organizations to determine the effects of EMP on different types of telecommunications equipment, facilities, and operations by:
  - The testing and analysis of new technologies introduced into telecommunications networks that will support NS/EP services prior to widespread introduction into the public network. IP-related equipment should be a major near-term focus of this testing and analysis. This analysis should include examining the use of standards in terms of prevention and mitigation benefits.
  - Capturing the lessons learned from future outages associated with the expected growth of voice communications by nontraditional carriers and the tremendous growth in wireless communications. It is important that such lessons learned be captured in a systematic and fiscally prudent manner.

Historically, data captured by the Federal Communications Commission (FCC) on major outages has been extremely valuable in identifying and correcting problems as they are exhibited in deployed systems. Again, this is consistent with the EMP Commission's philosophy of preventing disastrous consequences from "cheap shot" attacks.

### ***Reducing the Effects of Power Outages on the Telecommunications Infrastructure***

In a power outage, telecommunications carriers typically depend on battery supplies that last from 4 to 8 hours and in some cases fixed and mobile generators that may have up to 72 hours of operating fuel. A key concern is the potential that major telecommunications facilities may not have primary power in the event of a long-term power outage of several weeks over a wide geographic area. Among the major concerns in such events are:

- ◆ The potential that major telecommunications facilities will not have prioritized access to fuel supplies on a long-term basis in the event of a long-term, wide-scale power outage.
- ◆ Facilities running on backup generators on a long-term basis will eventually require maintenance.

---

<sup>8</sup> AT&T (Albert Lewis) correspondence with FCC, May 13, 1998; MCI (Bradley Stillman) correspondence with FCC, December 8, 1999.

<sup>9</sup> 47 CFR Part 215 designated the Executive Agent, NCS, as the focal point within the Federal Government for all EMP technical data and studies concerning telecommunications.

These concerns proved prescient when Hurricane Katrina struck in August 2005. Katrina caused a prolonged blackout that resulted in telecommunications failures precisely because of the above concerns regarding fuel supplies and maintenance for emergency generators.

After the August 2003 Northeast blackout, recommendations were put forward by the NRIC to help address this power dependency issue. As part of lessons learned discussed in an August 27, 2003, NRIC presentation on the impact of the 2003 Northeast blackout, telecom-specific references were made to re-evaluate the Telecommunications Electric Service Priority (TESP) program: “Power management and restoral practices at the tactical level are under review by carriers—may need modifications to the TESP program to mitigate additional risks,” and “Development of TESP program for cellular networks to address priority restoration of critical cellular communications facilities is needed.”<sup>10</sup> TESP promotes (on a voluntary basis) the inclusion of critical telecommunications facilities in electric service providers’ priority restoration plans.<sup>11</sup>

Lessons learned from Katrina and the NRIC evaluation of the 2003 Northeast blackout form the underpinning for the following EMP Commission recommendations:

- ◆ Improve the ability of telecommunications to withstand the sustained loss of utility-supplied electric power:
  - Task the NCS and the North American Electric Reliability Corporation (NERC), or its successor, with providing, at a minimum, biannual status reports on the need for/adequacy of priority restoration of electric power by power utilities to selected telecommunications sites.
  - Task the Department of Energy (DOE) with exploring the adequacy of financial incentives to spur analysis of alternative powering sources that offer cost-effective and viable alternatives for telecom asset powering. For example, carriers are exploring new technologies such as fuel cells to support the powering of offices.

### ***Adequately Addressing Interdependency Impacts in Contingency Planning***

The potential impact of other interdependency effects, with a priority on NS/EP services, must be considered in any analysis of recovery planning. For example, the assumption of key personnel access to transportation to operations center sites or remote access to equipment should be addressed in contingency planning. With this in mind, the NCS would be a logical organization to address this area for critical national infrastructures. Specifically, the Commission recommends the following:

- ◆ Expand the role of the NCS within the Code of Federal Regulations (CFR) Part 215 (Federal Focal Point for EMP Information) to address infrastructure interdependencies related to NS/EP telecommunications services.

Supporting this recommendation is the need to exercise the National Response Framework to determine how well the plan addresses simultaneous degradation of multiple infrastructures. Industry personnel have suggested to the EMP Commission that a tabletop exercise considering this type of scenario would be extremely useful. Exercise results should be factored into the development of an EMP scenario to be included on the DHS list of National Planning Scenarios. Such an exercise would be invaluable in

<sup>10</sup> Aduskevicz, P., J. Condello, Capt. K. Burton, Review of Power Blackout on Telecom, NRIC, August 27, 2003, quarterly meeting.

<sup>11</sup> Homeland Security Physical Security Recommendations for Council Approval, Letter to Richard C. Notebaert, March 5, 2003.

understanding the impacts of telecommunications failures on other infrastructure sectors and vice versa. Of particular concern is the impact of losing telecommunications on the operating effectiveness of Supervisory Control and Data Acquisition (SCADA) systems for infrastructures such as electric power and natural gas.

Specifically, the Commission recommends the following:

- ◆ Task DHS with developing exercises and an additional National Planning Scenario incorporating a large-scale degradation for multiple infrastructures over a wide geographic area as might occur in an EMP event.

***Improving the Ability of Telecommunications Networks That Support Nationally Critical Applications to Survive EMP by Protecting Key Assets and Conducting Vulnerability Assessments***

The Commission recommends the following:

- ◆ Task NCS to identify key telecommunications network assets whose degradation can result in the loss of service to a large number of users. These might include next-generation routing and transport equipment and wireless network elements such as HLRs and Visiting Location Registers (VLRs). Cellular base stations should be part of this analysis.
- ◆ Task NCS through DHS, in accordance with the CFR for Telecommunications Electromagnetic Disruptive Effects (TEDE) affecting NS/EP telecommunications, to work with government and multiple industries (e.g., Federal Reserve Board and BITS [financial services], Federal Energy Regulatory Commission [FERC] and NERC [electric power], and DHS and first responders [civilian restoration]) to determine whether a high-reliability telecommunications service or services supporting mission-critical applications is needed. If so, consider partial federal funding for this service.
- ◆ Establish a reporting process to be developed by the FCC, NCS, and the telecommunications industry for reporting major outages from wireless, data communications, and Internet carriers to the FCC, analogous to what is done for wireline carriers, thereby capturing lessons learned.



## Chapter 4. Banking and Finance

### Introduction

The financial services industry comprises a network of organizations and attendant systems that process instruments of monetary value in the form of deposits, funds transfers, savings, loans, and other financial transactions. Virtually all economic activity in the United States (U.S.) and other developed countries depends on the functioning of the financial services industry. National wealth is the sum of all economic value, as reflected in part in existing capital and financial transactions. Most simply, the financial services industry is the medium and record keeper for financial transactions and repository of national, organizational, and individual wealth.

Today, most significant financial transactions are performed and recorded electronically; however, the ability to carry out these transactions is highly dependent on other elements of the national infrastructure. According to the President's National Security Telecommunications Advisory Committee (NSTAC), "The financial services industry has evolved to a point where it would be impossible to operate without the efficiencies of information technology and networks."<sup>1</sup>

The automation of the financial services industry has spurred the growth of wealth by increasing greatly the amount of business that can be conducted on a daily basis. For example, "in the early 1970s, the New York Stock Exchange [NYSE] closed every Wednesday to clear backlogs from an average daily trading volume of 11 million shares."<sup>2</sup> Today, the Securities Industry Automation Corporation (SIAC) has no interruption in exchange operations and routinely handles an average daily trading volume of more than 3 billion shares.<sup>3</sup>

"SIAC is responsible for providing the highest quality, most reliable and cost-effective systems to support the current and future business needs of the New York Stock Exchange"<sup>4</sup> and other institutions. "SIAC's Shared Data Center alone is linked to the securities industry by more than a thousand communications lines over which an average of 70 billion bytes of data is transmitted daily."<sup>5</sup> SIAC's Secure Financial Transaction Infrastructure, "improves the overall resilience of the financial industry's data communications connectivity...and offers firms reliable access to... trading, clearing and settlement, market data distribution, and other services."<sup>6</sup>

The technological revolution has not been limited to giant corporations. The individual consumer has witnessed the growth of convenient, on-demand money-dispensing

---

<sup>1</sup> United States, The President's National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report* (Washington, 1997), 4.

<sup>2</sup> Ibid.

<sup>3</sup> "Firsts and Records," NYSE Euronext, New York Stock Exchange Euronext, <http://www.nyse.com/about/history/1022221392987.html>.

<sup>4</sup> Network General Corporation, Securities Industry Automation Corporation — SIAC: Sniffer Distributed, San Jose, 2005, 1.

<sup>5</sup> Ibid.

<sup>6</sup> Boston Options Exchange, Telecom Connections, August 3, 2003, <http://www.bostonoptions.com/conn/tel.php>.



automated teller machines (ATM) in the United States from less than 14,000 in 1979<sup>7</sup> to more than 371,000 in 2003.<sup>8</sup>

The trend in the U.S. financial infrastructure is toward ever more sophisticated and powerful electronic systems capable of an ever increasing volume and velocity of business. The increasing dependence of the United States on an electronic economy, so beneficial to the management and creation of wealth, also increases U.S. vulnerability to an electromagnetic pulse (EMP) attack.

For example, the terrorist attacks of September 11, 2001, demonstrated the vulnerabilities arising from the significant interdependencies of the Nation's critical infrastructures. The attacks disrupted all critical infrastructures in New York City, including power, transportation, and telecommunications. Consequently, operations in key financial markets were interrupted, increasing liquidity risks for the U.S. financial system.<sup>9</sup>

An interagency paper jointly issued by the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), and the Securities and Exchange Commission (SEC), specifies clearing and settlement systems as the most critical business operations at risk for financial markets.<sup>10</sup> Because financial markets are highly interdependent, a wide-scale disruption of core clearing and settlement processes would have an immediate systemic effect on critical financial markets.<sup>11</sup>

Moreover, in December 2002, the FRB revised its policy and procedures for national security and emergency preparedness telecommunications programs administered by the National Communications System (NCS) to identify those functions supporting the Federal Reserve's national security mission to maintain national liquidity.<sup>12</sup> The FRB expanded the scope of services that would seriously affect continued financial operations if a telecommunications disruption of "a few minutes to one day" occurred.<sup>13</sup> These functions, which are listed below, "require same-day recovery and are critical to the operations and liquidity of banks and the stability of financial markets".<sup>14</sup>

- ◆ Large-value interbank funds transfer, securities transfer, or payment-related services
- ◆ Automated clearing house (ACH) operators
- ◆ Key clearing and settlement utilities
- ◆ Treasury automated auction and processing system

<sup>7</sup> United States, The President's National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report* (Washington, 1997), 47.

<sup>8</sup> ATM & Debit News, September 10, 2003, ATM & Debit News Survey Data Offers Insight into Debit Card and Network Trends in Its 2004 EFT Data Book, press release, <http://www.sourcemediacom/pressreleases/20030910ATM.html>.

<sup>9</sup> MacAndrews, James J., and Simon M. Potter, "Liquidity Effects of the Events of September 11, 2001," Federal Reserve Bank of New York Economic Policy Review, November 2002.

<sup>10</sup> The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (Washington: GPO, 2002), 5.

<sup>11</sup> Systemic risk includes the risk that failure of one participant in a transfer system or financial market to meet its required obligations will cause other participants to be unable to meet their obligations when due, causing significant liquidity or credit problems or threatening the stability of financial markets. The use of the term "systemic risk" in this report is based on the international definition of systemic risk in payments and settlement systems provided in Committee on Payment and Settlement Systems, Bank for International Settlements, "A Glossary of Terms in Payment and Settlement Systems," 2001.

<sup>12</sup> "Federal Reserve Board Sponsorship for Priority Telecommunications Services of Organizations That Are Important to National Security/Emergency," *Federal Register*, 67:236 (December 9, 2002), 72958.

<sup>13</sup> Ibid.

<sup>14</sup> Ibid.

- ◆ Large-dollar participants of these systems and utilities.<sup>15</sup>

The increasing dependence of the United States on an electronic economy also adds to the adverse effects that would be produced by an EMP attack. The electronic technologies that are the foundation of the financial infrastructure are potentially vulnerable to EMP. These systems are also potentially vulnerable to EMP indirectly through other critical infrastructures, such as the electric power grid and telecommunications.

### The Financial Services Industry

In a December 1997 study, *Financial Services Risk Assessment Report*, NSTAC described the financial services industry as comprising four sectors. This definition is reflected or shared in current U.S. government reports, regulations, and legislation that treat the financial services industry as having these components:

- ◆ Banks and other depository institutions
- ◆ Investment-related companies
- ◆ Industry utilities
- ◆ Third-party processors and other services.

*Banks and Other Depository Institutions.* In 2004, U.S. banks held more than \$9 trillion<sup>16</sup> of domestic financial assets, and investment companies and other private institutions held about \$17 trillion of the national wealth.<sup>17</sup> Banks and other depository institutions, including thrifts, credit unions, and savings and loan associations, are vital to the functioning of the economy. These institutions hold and provide access to deposits, provide loans, transfer funds, promote savings, and facilitate economic growth.

Commercial banks are the repository of the most financial assets of any depository institution. Commercial banks disseminate financial information, act as agents in buying and selling securities, serve as trustees for corporations or individuals, transfer funds, collect deposits, and provide credit. The top 10 commercial banks control nearly half of all assets held by banks.<sup>18</sup>

Credit unions, savings and loan associations, and savings banks generally are referred to as “other depository institutions.” These institutions usually service households instead of businesses. Credit unions are the most financially significant of these institutions. By the end of 2004, credit unions had more than 85 million members and managed more than \$668 billion in assets.<sup>19</sup>

The single most important banking institution is the Federal Reserve System. Established by the U.S. Congress in 1913, the Federal Reserve System is the central bank of the United States. This system does not deal directly with the general public, but with other banks. It is, in essence, the Nation’s bank for commercial banks.

The primary purpose of the Federal Reserve System is to maintain the stability, safety, and flexibility of the financial system and contain systemic risk that may arise in the

---

<sup>15</sup> Ibid.

<sup>16</sup> United States, Federal Reserve Board, *Federal Reserve Bulletin Statistical Supplement* (Washington: GPO, 2004), 15.

<sup>17</sup> Investment Company Institute, *2005 Investment Company Factbook*, 2005, <http://www.ici.org/factbook>.

<sup>18</sup> Klee, Elizabeth C., and Fabio M. Natalluci, “Profits and Balance Sheet Developments at U.S. Commercial Banks in 2004,” *Federal Reserve Bulletin*, Spring 2005:144.

<sup>19</sup> United States Credit Union Statistics, Credit Union National Association, 2004, [http://advice.cuna.org/download/us\\_totals.pdf](http://advice.cuna.org/download/us_totals.pdf).

financial markets. The Federal Reserve accomplishes this mission by establishing monetary policy, by servicing financial institutions and other government agencies, and by regulating and supervising banks.

As the central bank of the United States, the Federal Reserve System extends emergency credit to commercial banks and controls interest rates, foreign exchange, and the money supply. The Federal Reserve also performs check-clearing and processing and transfer of government securities and funds between financial institutions.

Federal Reserve System banks are supervised by a Board of Governors who are appointed by the president and confirmed by the U.S. Senate; however, the banks are owned by private member banks. For administrative purposes, the United States is divided into 12 Federal Reserve Districts, each district served by a Federal Reserve Bank. The 12 Federal Reserve Banks are located in New York, Boston, Philadelphia, Richmond, Atlanta, Cleveland, Chicago, St. Louis, Kansas City, Dallas, Minneapolis, and San Francisco.

*Investment-Related Companies.* Unlike commercial banks, underwriters, brokerages, and mutual funds are not depository institutions. Rather, these institutions provide a wide range of services to institutional and individual investors. They act as intermediaries in pooling investments by a large group of customers and in market trades.

Investment banks and underwriters finance investments by government and commercial enterprises through stocks and bonds. Investment banks also arrange mergers. Currently, the largest 50 firms hold 90 percent of the market share.<sup>20</sup>

Brokerages help investors by acting as agents or intermediaries with commodities and securities markets. Brokerages advise clients, perform research, and place trades. "The securities brokerage industry in the United States includes fewer than 400 companies with combined annual revenue of over \$100 billion. The top 50 companies hold over 80 percent of the market share."<sup>21</sup>

Mutual funds pool money from many people and institutions and invest it in stocks, bonds, or other securities. A portfolio manager is employed by the mutual fund to achieve its financial objective, such as providing a reliable source of investment income or maximizing long-term returns. The mutual fund market is dominated by 25 companies. The top five companies hold one-third of the market. The mutual fund industry holds about \$8.1 trillion dollars in assets.<sup>22</sup>

*Industry Utilities.* Banks, including the Federal Reserve System, and investment-related companies, such as investment banks, brokerages, and mutual funds, all rely on industry utilities to transact business. Financial service utilities are the institutions that provide a common means for transferring, clearing, and settling funds, securities, and other financial instruments, as well as exchanging financial information.

Financial industry utilities have largely replaced paper transactions with electronic means. Check and cash transactions are still the largest number of financial transactions in the national economy. However, paper transactions are vastly surpassed in total value

---

<sup>20</sup> "Industry Overview: Investment Banking," Hovers, Inc.,  
[http://www.hoovers.com/investment-banking/--ID\\_209--/free-ind-fr-profile-basic.xhtml](http://www.hoovers.com/investment-banking/--ID_209--/free-ind-fr-profile-basic.xhtml).

<sup>21</sup> Ibid.

<sup>22</sup> Investment Company Institute, *2005 Investment Company Factbook*, 2005, 59,  
[http://www.ici.org/factbook/pdf/05\\_fb\\_table01.pdf](http://www.ici.org/factbook/pdf/05_fb_table01.pdf).

by electronic transactions through wire transfers, interbank payment systems, ACHs, and clearing and settlement systems for securities and other investments.

Modern financial services utilities have transformed the national economy from a paper system into an electronic system. Examples of some key industry utilities include FEDNET, Fedwire, ACH, Clearing House Interbank Payments System (CHIPS), the Society for Worldwide Interbank Financial Telecommunications (SWIFT), the National Association of Securities Dealers' Automated Quotation System (NASDAQ), the NYSE, the New York Mercantile Exchange (NYMEX), and the Depository Trust and Clearing Corporation (DTCC).

FEDNET is a communications system connecting all 12 Federal Reserve Banks nationwide and the financial services industry generally. FEDNET transfers funds in real time among banks and other depository institutions, performs real-time sales and record keeping for the transfer of government securities, and serves as ACH.

Fedwire is the primary national network for the transfer of funds between banks; the system currently serves approximately 7,500 institutions. Fedwire's book-entry securities transfer application allows banks and other depository institutions to transfer U.S. government securities. This network has enabled the Federal Reserve to largely replace paper U.S. government securities with electronic book entries. Transfers performed on Fedwire are irrevocable upon receipt and are settled immediately. The average value of a Fedwire funds transaction is about \$3.9 million dollars.<sup>23</sup> In 2005, Fedwire processed an average daily volume of approximately 528,000 payments, with an average daily value of about \$2.1 trillion.<sup>24</sup>

ACH was developed in the 1970s as an alternative to the traditional paper-based system for clearing checks. ACH electronic transactions include direct deposits of payrolls, pensions, benefits, and dividends and direct bill payments. The Federal Reserve annually processes about 36.7 billion ACH payments valued at \$39.9 trillion dollars.<sup>25</sup>

CHIPS is an electronic system for interbank transfer and settlement. CHIPS is the primary clearing system for foreign exchange. "It processes over 285,000 payments a day with a gross value of \$1.4 trillion." This includes 95 percent of all international U.S. dollar payments.<sup>26</sup>

The SWIFT provides stock exchanges, banks, brokers, and other institutions with a cost-effective, secure international payment message system. These messages are instructions between banks and other institutions regarding payments and transfers, not payments themselves. SWIFT carries approximately 8 million messages daily.<sup>27</sup>

The NASDAQ and the NYSE are the largest securities markets. NASDAQ is an electronic communications network that consolidates the quotations of multiple dealers, displayed in real time, and allows electronic trading. The NYSE offers similar electronic

---

<sup>23</sup> Federal Reserve Board, <http://www.federalreserve.gov/paymentsystems/coreprinciples/default.htm#fn12>.

<sup>24</sup> Ibid.

<sup>25</sup> United States, Federal Reserve System, *Analysis of Noncash Payments Trends in the United States: 2000–2003* (Washington: 2004), 5.

<sup>26</sup> SWIFT, *2005 Annual Report: Alternative Connectivity for CHIPS Reinforces Resilience*, [http://www.swift.com/index.cfm?item\\_id=59677](http://www.swift.com/index.cfm?item_id=59677).

<sup>27</sup> SWIFT, *2004 Annual Report: SWIFTnet Now the Benefits Really Begin*, [http://www.swift.com/index.cfm?item\\_id=56868](http://www.swift.com/index.cfm?item_id=56868).

services. NASDAQ executed 957.9 million trades valued at more than \$3.7 trillion dollars in 2004, and the NYSE traded a slightly lesser amount.<sup>28</sup>

The NYMEX trades on futures contracts such as unleaded gasoline, heating oil, crude oil, natural gas, and platinum. NYMEX typically conducts crude oil transactions involving the total daily production of the entire world.

The DTCC settles securities trades for participant banks and is the largest securities depository in the world. In 2004, the company completed financial settlement for a quadrillion dollars in securities transactions. DTCC keeps records on securities and conducts transactions electronically. Annually, DTCC participants deliver securities valued at about \$4.5 trillion to DTCC to make electronic records of ownership.<sup>29</sup>

*Third-Party Processors and Other Services.* Third-party processing companies are technology companies that provide electronic processing services to financial institutions. Banks and other financial institutions can cut overhead by contracting with third parties to perform the mechanics of electronic transactions. Technology-related outsourcing is especially appealing because of dynamic changes in technology. The high cost and complexity of new technologies has driven many banks into partnerships with third-party specialists in the field of electronic finance. Services typically offered by third-party processors include data center management, network management, application development, check and statement processing, mutual fund account processing, and electronic funds transfer.

### **Vulnerability to EMP**

The financial infrastructure is highly dependent on electronic systems, which should be clear from the preceding discussion. Virtually all transactions involving banks and other financial institutions happen electronically. Virtually all record keeping of financial transactions are stored electronically. Just as paper money has replaced precious metals, so an electronic economy has replaced the paper one. The financial infrastructure is a network of simple and complex electronic machinery, ranging from telephones to main-frame computers, from ATMs to vast data storage systems.

The electronic technologies that are the foundation of the financial infrastructure are potentially vulnerable to EMP. These systems also are potentially vulnerable to EMP indirectly through other critical infrastructures, such as the power grid and telecommunications.

The financial services industry and knowledgeable experts on the security of that industry judge that the industry is highly robust against a wide range of threats. The NSTAC, for example, notes that the leading financial institutions take a multilayered approach to building robustness and recoverability into their systems:

*Operational data centers are engineered from the ground up with survivability in mind. Some are hardened with thick concrete walls and protected with extensive perimeter security measures equivalent to military command posts. Most have uninterruptible power supplies, generators, and on-site fuel*

<sup>28</sup> NASDAQ, *NASDAQ Announces Market Year-end Statistics for 2004*, <http://ir.nasdaq.com/releasedetail.cfm?ReleaseID=177077>.

<sup>29</sup> DTCC, *2004 Annual Report: What is a Quadrillion?* 3, [http://www.dtcc.com/downloads/annuals/2004/2004\\_report.pdf](http://www.dtcc.com/downloads/annuals/2004/2004_report.pdf).



*storage sufficient to allow the facility to run independently of the power grid ranging from a few hours to over a month. External telecommunications links are diversely homed, with multiple building access points and connections to more than one central office...wherever possible. Operational procedures within the data center are designed to minimize the risk of human errors causing interruptions, and most or all data files are copied and stored on disk or tape at off-site facilities.*<sup>30</sup>

NSTAC also observes that, “Numerous natural and man-made disasters...have forced financial institutions to test and refine their disaster recovery capabilities.”<sup>31</sup> The financial services industry’s dependence on other infrastructures has been tested in real emergencies. For example, in 1988, a fire in the Ameritech central office in Hinsdale, Illinois, disabled long-distance telecommunications for the Chicago Board of Trade and other major institutions. Wall Street was blacked out for nearly a week by an electrical fire in a Consolidated Edison office in August 1990. In April 1992, underground flooding in Chicago caused sustained telecommunication and power outages. Financial institutions faced widespread electrical power outages in the West during the summer of 1996 and in the Northeast during the summer of 2003.

“In addition,” according to NSTAC, “the industry weathered one of the worst terrorist attacks in recent history”:

*The World Trade Center bombing on February 26, 1993, struck at the industry’s heart, affecting the New York Mercantile Exchange and many securities dealers and otherwise disrupting activities throughout Wall Street. Numerous problems with facilities, systems, procedures, and staffs were encountered as firms scurried to recover, and some securities firms’ operations were shut down temporarily. However, none of the most critical services were affected, and the effect on the economy as a whole was minimal.*<sup>32</sup>

The financial services industry also weathered the more devastating terrorist attack on September 11, 2001, that destroyed the World Trade Center. NSTAC found that these types of events, “led to improved robustness of the financial services infrastructure.”

NSTAC’s judgment that the financial services industry enjoys robust survivability against a wide range of threats is seconded by the National Academy of Sciences (NAS) in its study, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (2002). According to the NAS, the U.S. financial infrastructure is highly secure because of the redundancy of its electronic systems: “While no law of physics prevents the simultaneous destruction of all data backups and backup facilities in all locations, such an attack would be highly complex and difficult to execute, and is thus implausible.”<sup>33</sup>

<sup>30</sup> United States, The President’s National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report* (Washington, 1997), 40.

<sup>31</sup> Ibid.

<sup>32</sup> Ibid.

<sup>33</sup> National Academies of Science, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington: National Academies Press, 2002), 137.



However, the NSTAC and NAS studies were focused primarily on the threat to the financial services industry from cyberterrorists using computer-based attacks. These studies did not evaluate the threat from EMP attack.

An EMP attack would pose the very kind of simultaneous and widespread threat postulated by the NAS that would be fatal to the financial infrastructure but judged by them to be too difficult to execute and implausible for cyberterrorists. EMP effects propagate at the speed of light and would cover a broad geographic area. Such an attack potentially could achieve the NAS criteria for financial infrastructure catastrophe: “simultaneous destruction of all data backups and backup facilities in all locations.”<sup>34</sup>

An EMP would probably not erase data stored on magnetic tape. However, by shutting down power grids and damaging or disrupting data retrieval systems, EMP could deny access to essential records stored on tapes and compact discs (CD). Moreover, because EMP physically destroys electronic systems, it is also in the category of threats that NSTAC concludes are more worrisome than cyberterrorism: “Physical attacks remain the larger risk for the industry.”

The vast majority of electronic systems supporting the financial infrastructure have never been tested, let alone hardened, against EMP. Yet the enormous volume, speed, and accuracy required of the electronic infrastructure supporting the financial services industry allow little or no room for error. Financial operations could not tolerate the kind of disruptions or mass systemic destruction likely to follow an EMP attack.

For example, CHIPS interbank transactions typically involve about \$1.4 trillion dollars of business every day, or some \$182 billion dollars every hour.<sup>35</sup> CHIPS and Fedwire routinely receive 5 to 10 funds transfer messages each second during peak traffic periods.<sup>36</sup> The Options Clearing Corporation manages \$1.05 billion in average daily premium settlements.<sup>37</sup> On Christmas Eve 2004, a single credit card association processed over 5,000 transactions per second.<sup>38</sup> Financial institutions also must store tremendous amounts of data. Terabyte portfolios (containing 1 trillion bytes) are now common, and some databases exceed a petabyte (1,000 trillion bytes). Changes in these huge databases must be recorded at the end of every business day.

“Dealing with this kind of volume, industry utilities cannot afford any interruption in service,” according to NSTAC. An EMP attack, with its potential to disrupt communications possibly for days, weeks, or months and to destroy or change databases, would place the financial infrastructure at risk.

Although the financial services industry has survived and learned from natural and man-made disasters, those disasters also have exposed vulnerabilities that could be exploited by an EMP attack. According to the staff director for management of the FRB, the terrorist attack of September 11, 2001, on the World Trade Center exposed telecommunications and the concentration of key facilities as serious weaknesses of the financial

<sup>34</sup> Ibid.

<sup>35</sup> SWIFT, 2005 Annual Report: Alternative Connectivity for CHIPS Reinforces Resilience, [http://www.swift.com/index.cfm?item\\_id=59677](http://www.swift.com/index.cfm?item_id=59677).

<sup>36</sup> Ibid.

<sup>37</sup> One Chicago (April 30, 2002), ONECHICAGO, Options Clearing Corporation and Chicago Mercantile Exchange, Inc., Sign Clearinghouse Agreements, press release, [http://www.onechicago.com/060000\\_press\\_news/press\\_news\\_2002/04302002.html](http://www.onechicago.com/060000_press_news/press_news_2002/04302002.html).

<sup>38</sup> “Digital Transactions News,” *Digital Transactions*, January 6, 2005, MasterCard Worldwide, Digital Transactions, <http://www.digitaltransactions.net/newsstory.cfm?newsid=466>.

services industry. Equity markets closed for 4 days, until September 15, due to failed telecommunications. The NYSE could not reopen because key central offices were destroyed or damaged, leaving them unable to support operations. According to this senior government official, Fedwire, CHIPS, and SWIFT would cease operation if telecommunications were disrupted. He further observed that ACH, ATMs, and credit and debit cards all depend on telecommunications. Disruption of these systems would force consumers to revert to a cash economy.<sup>39</sup>

Further, response to the Northeast power outage in August 2003 has been depicted as a triumph for the financial services industry safeguards implemented since the terrorist attacks of September 11, 2001. But this is not the whole picture. Some analysts observe that the blackout happened under nearly ideal conditions to facilitate financial industry recovery. The blackout happened on a Thursday at 4:10 p.m., after the 4:00 p.m. closing time for financial markets, and it was largely over for the financial industry by 9:00 a.m. the following Friday morning. Business was also light, at its nadir, as is usual during August.

Even so, recovery from the 2003 blackout still required many in the financial industry to work overnight. The American Stock Exchange did not open because its air conditioners would not operate. Many traders could not get to work on Friday because the transportation system was paralyzed. Some companies were unable to reach the NASDAQ electronic exchange by telephone. Many ATMs failed. Many of the 1,667 banks in New York City closed on Friday because of continuing power outage. Many industries with back-up generators, like KeyCorp in Cleveland, were unprepared for a blackout that lasted for more than a few hours, and they had difficulty getting diesel fuel.

The fortunate timing and short duration of the 2003 blackout affected the financial industry for a relatively brief period. Nonetheless, banks had to compensate for financial imbalances by borrowing \$785 million dollars from the Federal Reserve System. This was 100 times the amount borrowed the previous week, and the greatest amount borrowed since the week after the September 11 attacks.<sup>40</sup> Most economists concur that the blackout had a small but measurable effect on the U.S. third-quarter economic growth.

These observations suggest that, if an EMP attack were to disrupt the financial industry for days, weeks, or months rather than hours, the economic impact would be catastrophic. The prolonged blackout resulting from Hurricane Katrina in August 2005 is a far better example than the Northeast blackout of 2003 of the challenge that would be posed to the financial infrastructure from EMP. The Katrina blackout, comparable to a small EMP attack, disrupted normal business life for months and resulted in a staggering economic loss that is still an enormous drain on the national economy.

The financial network is highly dependent on power and telecommunications for normal operations. Widespread power outages would shut down the network, and all financial activity would cease until power was restored, as happened during Hurricane Katrina. Even if power were unaffected or restored in short order, full telecommunications are required to fully enable the financial network. If critical elements within the telecommunications infrastructure were negatively affected by the EMP attack (i.e., at main and

<sup>39</sup> Malphrus, Steve, Staff Director for Management, Federal Reserve Board, personal communication.

<sup>40</sup> Jackson, William D., *Homeland Security: Banking and Financial Infrastructure Continuity*, U.S. Congress, March 16, 2004, Congressional Research Service (Washington, 2004), 6, <http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL3187303162004.pdf>.

local switches), the financial network would be impacted negatively to some degree and consequently be highly dependent on the telecommunication recovery timelines before it could be brought back online with the required capability and capacity.

The extent to which the financial network is able to function as it is being brought back online will be highly dependent on the level of damage incurred by the network as a result of the EMP attack.

### **Consequences of Financial Infrastructure Failure**

Despite the robustness of U.S. financial infrastructures against a wide range of threats, they were not designed to withstand an EMP attack. Indeed, the highly sophisticated electronic technologies that make the modern U.S. financial infrastructure possible are the components most vulnerable to EMP.

An EMP attack that disrupts the financial services industry would, in effect, stop the operation of the U.S. economy. Business transactions that create wealth and jobs could not be performed. Loans for corporate capitalization and for private purposes, such as buying homes and automobiles could not be made. Wealth, recorded electronically in bank databases, could become inaccessible overnight. Credit, debit, and ATM cards would be useless. Even reversion to a cash economy might be difficult in the absence of electronic records that are the basis of cash withdrawals from banks. Most people keep their wealth in banks and have little cash on hand at home. The alternative to a disrupted electronic economy may not be reversion to a 19th century cash economy, but reversion to an earlier economy based on barter.

In the immediate aftermath of an EMP attack, banks would find it very difficult to operate and provide the public with the liquidity they require to survive; that is, to buy food, water, gas, or other essential supplies and services. Modern banking depends almost entirely on electronic data storage and retrieval systems for record keeping and to perform account transactions. An EMP attack that damages the power grid or electronic data retrieval systems would render banking transactions virtually impossible as a practical or legal matter.

Operating a banking system using paper and handwritten transactions would be difficult without access to the information contained in electronic records. If a makeshift paper banking system could be organized on an emergency basis, such a system would be fraught with the risk of fraud, theft, and costly mistakes. Such a system would not be consistent with the cautious behavior and natural interest of banks in assigning highest priority to protecting financial assets. Protocols and business standards that are required of banks under their charters for insurance purposes and to protect them from legal liability assume the existence of modern electronic banking systems and the reliability, redundancy, and surety that such systems provide.

A survey by Commission staff of natural and man-made disasters found no case in which banks, bereft of their electronic systems because of blackout, reopened their doors and did business by hand. Unless banks have well-prepared contingency plans in place to revert to paper and handwritten transactions in advance of a crisis, it is very doubtful that bank managers would have the capability, authority, or motivation to attempt a paper and handwritten banking system in the aftermath of an EMP attack. Unless directed by federal authority to create contingency plans for operating without electricity, it is doubtful the business community would undertake such plans on its own.

In the aftermath of an EMP attack, individuals and corporations would have many sound reasons for being cautious, risk averse, and unwilling to resume business as usual. Once power, telecommunications, and transportation are restored, even if restored promptly, within a matter of days, psychological concerns that affect economic revitalization may linger. Full recovery will require restoring the trust and confidence of the business community in the infrastructures, in financial institutions, and in the future. The Great Depression outlasted its proximate causes by many years, despite strenuous efforts by the Federal Government to implement financial reforms and jump-start the economy, in part because businesses were unwilling to risk their capital in a system that had lost their confidence.

The Department of the Treasury and the SEC share the view that failure of electronic systems supporting the critical infrastructure for even one business day threatens the financial system with wide-scale disruption and risk to one or more critical markets. Indeed, the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, by the Department of the Treasury and the SEC advocates “the overall goal of achieving recovery and resumption within two hours after an event.” It states:

*In light of the large volume and value of transactions/payments that are cleared and settled on a daily basis, failure to complete the clearing and settlement of pending transactions within the business day could create systemic liquidity dislocations, as well as exacerbate credit and market risk for critical markets. Therefore, core clearing and settlement organizations should develop the capacity to recover and resume clearing and settlement activities within the business day on which the disruption occurs with the overall goal of achieving recovery and resumption within two hours after an event.*<sup>41</sup>

Partial or small-scale disruption of the financial infrastructure would probably be enough to bring about a major economic crisis. Nonfunctioning ATM machines, for example, and other impediments to obtaining cash might well undermine consumer confidence in the banking system and cause a panic. NSTAC observes that the ultimate purpose behind all the financial industry’s security efforts is to retain consumer confidence: “The ability of an institution to maintain the trust, and hence, the business, of its customers is viewed as an even greater value than the dollars and cents involved.”<sup>42</sup> A related NAS study concludes that an attack that destroys only electronic records would be “catastrophic and irreversible.”<sup>43</sup> Although it is highly unlikely that stored financial data on magnetic media would be damaged by EMP, the electronic systems for retrieving data are potentially vulnerable to EMP and are dependent on a vulnerable power grid. Data and essential records are useless if inaccessible. According to the NAS, “Irrecoverable

---

<sup>41</sup> U.S. Security Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, April, 2003.

<sup>42</sup> United States, The President’s National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report* (Washington, 1997), 27.

<sup>43</sup> National Academies of Science, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington: National Academies Press, 2002), 137.

loss of critical operating data and essential records on a large scale would likely result in catastrophic and irreversible damage to U.S. society.”<sup>44</sup>

### Recommendations

Securing the financial services industry from the EMP threat and from other threats is vital to the national security of the United States. The Federal Government must ensure that this system can survive sufficiently to preclude serious, long-term consequences.

The Department of Homeland Security, the FRB, and the Department of the Treasury, in cooperation with other relevant agencies, must develop contingency plans to survive and recover key financial systems promptly from an EMP attack.

Key financial services include the means and resources that provide the general population with cash, credit, and other liquidity required to buy essential goods and services. It is essential to protect the Nation’s financial networks, banking records, and data retrieval systems that support cash, check, credit, debit, and other transactions through judicious balance of hardening, redundancy, and contingency plans.

The Federal Government must work with the private sector to ensure the protection and effective recovery of essential financial records and services infrastructure systems from all deliberate adverse events, including EMP attack. Implementation of the recommendations made by the Department of the Treasury, the FRB, and the SEC in their *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* to meet sabotage and cyberthreats that could engender requirements for protection and recovery should be expanded to include expeditious recovery from EMP attack as follows:

- ◆ “Every organization in the financial services industry should identify all clearing and settlement activities in each critical financial market in which it is a core clearing and settlement organization or plays a significant role” that could be threatened by EMP attack.
- ◆ Industry should “determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets” following an EMP attack.
- ◆ Industry should be prepared to cope with an EMP attack by maintaining “sufficient geographically dispersed resources to meet recovery and resumption objectives.... Back-up sites should not rely on the same infrastructure components (e.g., transportation, telecommunications, water supply, electric power) used by the primary site. Moreover, the operation of such sites should not be impaired by a wide-scale evacuation at or inaccessibility of staff that service the primary site.”
- ◆ Industry should “routinely use or test recovery and resumption arrangements.... It is critical for firms to test back-up facilities of markets, core clearing and settlement organizations, and third-party service providers to ensure connectivity, capacity, and the integrity of data transmission” against an EMP attack.<sup>45</sup>

---

<sup>44</sup> Ibid.

<sup>45</sup> U.S. Security Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, April 2003.



## Chapter 5. Petroleum and Natural Gas

### Introduction

The United States economy is dependent on the availability of energy. While much of that energy originates in natural resources of coal, hydroelectric, and nuclear materials and is distributed to users through the electric power grid, more than 60 percent of all U.S. domestic energy<sup>1</sup> usage derives from petroleum (about 40 percent) and natural gas (more than 20 percent) and is distributed to users through an extensive national pipeline system. Refined petroleum products and natural gas power our cars, heat our homes, energize our factories, and comprise critical elements of industrial materials ranging from fertilizers to plastics, all enabling the normal functioning of our energy intensive civil society. In 2006, according to the Annual Energy Review, the United States imported an average of 10 million barrels of crude oil and 11.5 billion cubic feet of natural gas every day. Domestically the United States produced about 5 million barrels of crude and 50.6 billion cubic feet of dry gas daily. All of these energy resources were delivered from their points of production or ports of entry to users or further distribution points through the national pipeline system.

While the closely related petroleum and natural gas infrastructures comprise a variety of production, processing, storage, and delivery elements, as described in the next section, the focus of this chapter will be on the delivery system. In particular, we shall focus on the potential electromagnetic pulse (EMP) vulnerability of the more than 180,000 miles of interstate natural gas pipelines and the more than 55,000 miles of large — 8-inch to 24-inch diameter — oil pipelines.<sup>2</sup> We shall point to the potential vulnerabilities of the electronic control systems — supervisory control and data acquisition systems (SCADA) — that were discussed in general terms in Chapter 1, but whose criticality and centrality for the operation of the petroleum and natural gas infrastructure distribution systems are particularly prominent. Control system components with low voltage and current requirements, such as integrated circuits, digital computers, and digital circuitry, are ubiquitous in the U.S. commercial petroleum and natural gas infrastructures, and EMP-caused failures can induce dangerous system malfunctions resulting in fires or explosions.

### Infrastructure Description

#### Petroleum

The petroleum infrastructure can be divided into two parts: the upstream sector, which includes exploration and production of crude oil, and the downstream sector, which comprises the refining, transmission, and distribution of the finished petroleum product.

Physical components of the upstream sector include land oil wells and waterborne oil rigs for exploration, drilling, and extraction of crude oil. In 2006, there were 274 rotary rigs operating on- and off-shore in the United States and 501,000 crude oil producing wells (**figure 5-1**). In addition, many elements of the production of crude oil are located abroad, because the majority of U.S. oil is imported.

In contrast to the production stages of petroleum, the United States is the largest producer of refined petroleum products in the world. In 2006, 149 refineries were producing

---

<sup>1</sup> Annual Energy Review 2006, International Energy Agency.

<sup>2</sup> Pipeline 101, <http://www.pipeline101.com>.



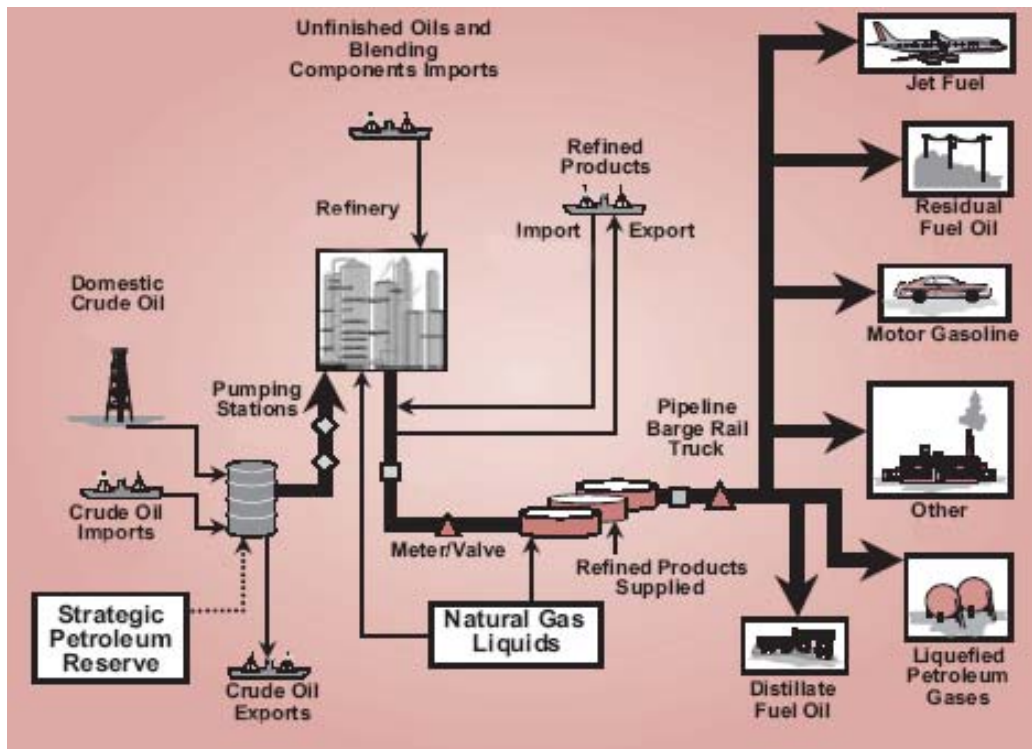


Figure 5-1. Petroleum Infrastructure<sup>3</sup>

approximately 23 percent of the world's refinery output. These refineries range in production capabilities from 5,000 barrels to approximately 500,000 barrels per day. Nearly one-half of America's refining capacity is located along the Gulf Coast, mostly in Texas and Louisiana. Other major refineries are found throughout the Midwest and in California, Washington, and along the East Coast of the United States.

The most pervasive physical element of the oil infrastructure is the extensive transmission network that moves crude oil from the field to the refineries for processing and brings the finished products to the consumer. Pipelines are the safest and most economical way to accomplish this and account for nearly 50 percent of all crude oil received in domestic refineries in 2006. Tankers transport an additional 46 percent of the crude oil received by refineries, with the remaining crude oil delivered to refineries by barge, rail tank car, and truck. There are approximately 55,000 miles of crude oil trunk lines (8-inch to 24-inch diameter) and an additional 30,000 to 40,000 miles of smaller gathering lines (2-inch to 6-inch diameter) across the United States. The trunk lines connect regional markets, while the smaller gathering lines transport crude oil from the well — on- or off-shore — to larger trunk lines and are located mainly in Texas and Louisiana. Movement of the refined products, such as gasoline, diesel, and jet fuel, to the marketplace is done largely by tankers. In addition, there are approximately 95,000 refined product pipelines nationwide, varying in diameter from 8 to 12 inches to 42 inches, that bring products to their final destinations.

Storage facilities are an integral part of the movement of oil by rail, highway, pipeline, barge, and tanker and can be aboveground, underground, or offshore. In the United

<sup>3</sup> National Petroleum Council, *Securing Oil and Natural Gas Infrastructures in the New Economy*, a Federal Advisory Committee to the Secretary of Energy, June 2001.

States, the most common storage tank is aboveground and made of steel plates. Most underground storage tanks are made out of steel as well. These storage facilities are located at each node in the production and distribution of petroleum and include tanks at the production field, marine terminals, refineries, pipeline pumping stations, retail facilities, car gasoline tanks, and home heating tanks.

In 2006, the United States imported about 60 percent of its petroleum consumption from abroad. Four thousand U.S. off-shore platforms, 2,000 petroleum terminals, and 4,000 oil tankers belonging to the world's energy trading nations and unloading petroleum at 185 ports in the United States, must also be counted as part of the petroleum infrastructure.

### **Natural Gas**

The natural gas infrastructure comprises production wells, processing stations, storage facilities, and the national pipeline system (see **figure 5-2**).

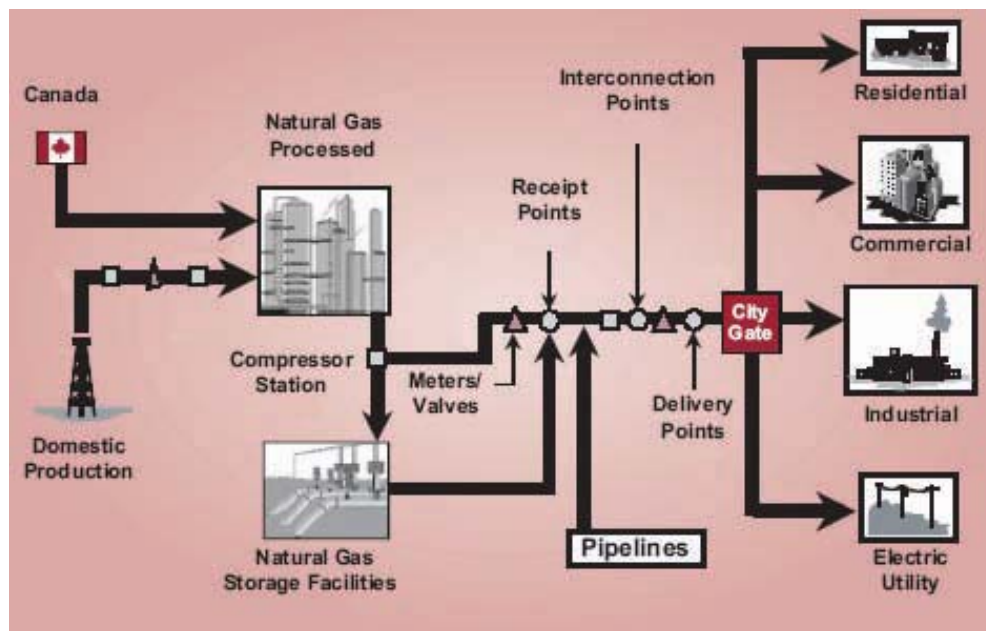


Figure 5-2. Natural Gas Infrastructure

In 2006, there were 448,461 gas- and condensate-producing wells<sup>4</sup> distributed among 63,353<sup>5</sup> oil and gas fields in the United States. There were more than 500 natural gas processing plants<sup>6</sup> and more than 1,400 compressor stations that maintain pressures in the pipeline and assure the forward motion of the transmitted gas supply. Storage facilities included 394 active underground storage fields, consisting of depleted oil and gas fields, aquifers, and salt caverns, five liquefied natural gas (LNG) import facilities, and 100 LNG peaking facilities. The pipeline system consists of more than 300,000 miles of interstate and intrastate transmission lines and an additional 1.8 million miles of smaller distribution lines that move gas closer to cities and to individual homes and business.

<sup>4</sup> Energy Information Administration, About Natural Gas, [http://www.eia.doe.gov/pub/oil\\_gas/natural\\_gas/analysis\\_publications/ngpipeline/transsys\\_design.html](http://www.eia.doe.gov/pub/oil_gas/natural_gas/analysis_publications/ngpipeline/transsys_design.html).

<sup>5</sup> Energy Information Administration, Oil and Gas Code Field Master List, 2006.

<sup>6</sup> Natural Gas Processing Plants, 1995-2004 EIA 6/2006.

Most of the natural gas consumed in the United States is produced domestically. Historically domestic production has accounted for around 85 percent of U.S. consumption with imports from Canada making up the remaining 15 percent. In recent years, domestic production has fallen to about 75 percent of consumption with the remainder imported from Canada. In 2005, five states — Texas, Oklahoma, Wyoming, Louisiana, and New Mexico — accounted for 77 percent of domestic natural gas production.

### **Direct Effects of EMP on Petroleum and Natural Gas Infrastructure**

The infrastructure described in the previous section is dependent on the continuous operation of a wide variety of electrical components: pumps to extract fuel from wells and manage its movement through pipelines, electrically driven systems to process materials in refineries, transportation systems to deliver fuels to users from storage sites, point-of-sale electronics to process transactions to retail customers, and so on — all of which represent potential points of vulnerability to an EMP pulse. We shall focus here on the vulnerability due to only one of these components — SCADA — because they represent a ubiquitous presence across all the different infrastructure elements and play a series of critical roles whose loss would severely compromise, or in some instances eliminate altogether, the ability of the infrastructure to function.

SCADA systems themselves, and their tested vulnerability to electromagnetic pulses, were described in some detail in Chapter 1, the introductory chapter to this volume, and we shall not repeat that here. Instead we describe the particular role of SCADAs within the petroleum and natural gas infrastructure, and then consider the consequences of an event which degrades or destroys the control and monitoring functions performed by the SCADAs.

### **Petroleum Infrastructure and SCADA**

SCADAs play a critical role at every stage of the oil industry's life cycle: production, refining, transportation, and distribution. Automation within the oil industry begins at the resource exploration stage and ends with final delivery to the customer. At each step, process control and SCADA are used not only to ensure that operations are efficient, but also that strict safety measures are maintained to prevent injuries and fatalities, fires and explosions, and ecological disasters.

SCADA systems, for example, are deployed in production fields, pipeline gathering systems, and along pipelines to monitor and adjust various operating parameters. These monitoring functions assist oil companies in preventing leaks and other hazardous conditions, as well as minimizing the impact of those that do occur.

These systems, which involve two-way traffic requiring paired channels, allow a master station to monitor and control the status of a multitude of measurements and tolerance limits at wellheads, pump stations, and valves, thus eliminating the need for constant manual surveillance. **Figure 5-3** presents a typical SCADA system for offshore oil production and onshore oil distribution, showing the use of remote terminal units (RTUs) and distributed control systems (DCS) at remote locations and their connection with the master terminal units (MTUs) through various communication media.

Pumping facilities that produce thousands of horsepower of energy and metering facilities that measure thousands of barrels per hour are routinely operated remotely via these SCADA systems. They can be properly operated only by using extremely reliable communications systems. The control aspect may include controls to a well pump to increase

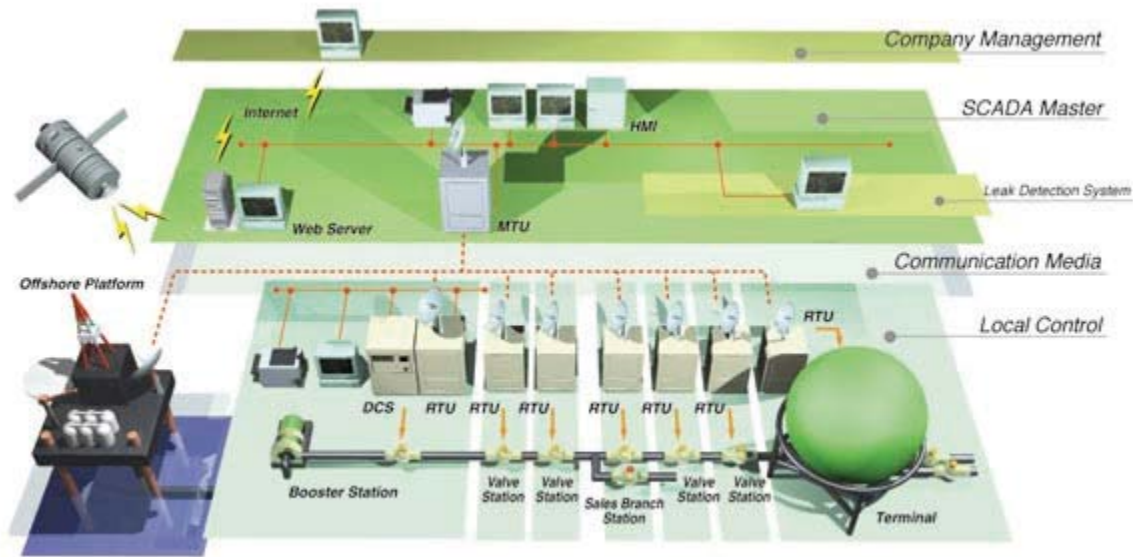


Figure 5-3. Typical SCADA Arrangement for Oil Operations

or decrease output or to shut down altogether. Pipeline controls may include changing routing, increasing or reducing the flow of the liquids or gases, and other functions. However, some pipeline facilities still require manual operation.

Process control is concerned with maintaining process variables, temperatures, pressures, flows, compositions, and the like at some desired operating value. Process control systems within refineries, along pipelines, and in producing fields were previously closed and proprietary. These control processes are now moving toward open architecture and commercially available software. The oil infrastructure now relies on e-commerce, commodity trading, business-to-business systems, electronic bulletin boards, computer networks, and other critical business systems to operate and connect the infrastructure. These assessment and control tools depend to a large degree on telecommunications and associated information technologies. Telecommunication in this context refers to a system of information linkages and data exchanges that include SCADA, the associated SCADA communication links, control systems, and integrated management information systems.

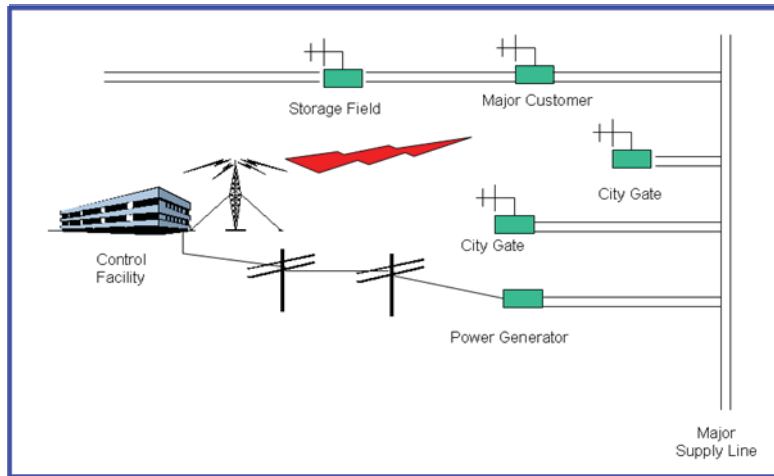
### Natural Gas Infrastructure and SCADA

SCADA is essential to modern natural gas operations. These systems provide the near-real-time data flows needed to operate efficiently in a deregulated environment. In addition, SCADA provides reporting of all transactions, establishing financial audit trails.

The key to effectively managing natural gas deliveries to customers is knowing what is happening along an interstate or intrastate pipeline system at all times. This is accomplished with Gas Control — a centralized command post that continuously receives information from facilities along the pipeline and disseminates information and operational orders to equipment and personnel in the field (see **figure 5-4**).

Through the use of SCADA equipment, Gas Control monitors volumes, pressures, and temperatures, as well as the operating status of pipeline facilities. Using microwave, telephone, or communication satellites, SCADA provides the Gas Control operator with information on the volume of natural gas flowing into the system and the volume of gas





**Figure 5-4. SCADA Integrates Control of Remote Natural Gas Facilities**

delivered to customers and gives the ability to quickly identify and react to equipment malfunctions or incidents. SCADA also gives Gas Control the capability to remotely start or stop compressors or open or close valves, thereby varying flow volumes to meet changes in customer demand for natural gas. Before the advent of SCADAs, all such functions, including tedious flow computations, were performed manually.

Automation of natural gas operations employs electronic components and technology to a high degree. Many of these components use simple mechanical or electrical properties to perform their defined roles, but an increasing number of them are computer-based. The major components and subsystems are RTUs, programmable logic controllers (PLC), MTUs, and communication systems, both wired and wireless. The total SCADA structure also includes control centers, information technology, personal computers (PC), and other peripheral technologies. RTUs and PLCs are usually located at the remote operational sites and connected to the MTUs and communication infrastructure through the communications network.

### **Effects of an EMP Event on the U.S. Petroleum and Natural Gas Infrastructures**

There are few empirical data to support definitive statements regarding the precise effects of an EMP event, should one occur. We can only extrapolate from what is known about the effects of various levels of EMP testing and what is indicated by other types of ongoing tests. It is evident that electronic devices, particularly those incorporating solid-state circuitry are, to varying degrees, susceptible to the effects of an EMP event.

The principal electronic components of a SCADA system, those devices most vulnerable to an EMP attack, are found in all the major subsystems of the SCADA installation. The MTU is a modern computer, with various solid-state circuits embedded on the microchips contained inside. An EMP event may affect these, either as a temporary disruption, which, if not automatically rebooted, might require manual intervention, or with permanent damage. If MTUs are not physically damaged, it may not be obvious whether their functional state has altered. As discussed earlier, loss of the MTU would blind the Control Center personnel to system data and performance. The physical system (e.g., pipelines, refineries) would continue to operate within the limits of the preprogrammed RTU controls, assuming that these components also have not been adversely affected by the EMP event.

The RTUs and PLCs used in today's SCADA systems rely on solid-state circuits to maintain their programming and to carry out the directives issued through those programs. This design makes the RTU and PLC inherently vulnerable to an EMP event. Although small, remote installations potentially have less exposure, it can be assumed that some or all of the RTUs and PLCs would be affected by an EMP event. As in the case of the MTU, affected embedded, integrated chips are suspect, even if the damage is not total and perhaps not immediately evident.

### **Gas**

Functional loss of the RTU and PLC results in loss of supervisory control at that location. The equipment is unable to direct changes in pressure to match changes in demand requirements for the natural gas sector. The gas delivery system should continue to operate, and natural gas should continue to flow, but ultimately the system may reach extreme conditions. Due to the presence of backup emergency pressure regulation, it is unlikely that such a failure would lead to an unsafe condition, one that would cause a rupture or explosion. The most likely result, given no manual intervention, would be significant loss of pressure after some period of time, leading to massive service disruption.

Currently, if any component of the control system (e.g., RTU, PLC, MTU) for the natural gas infrastructure fails, the system still has the mechanical ability to operate as it did in the days before SCADA. An EMP-induced false signal might affect operation if the signal unexpectedly closed a valve instead of keeping it open. The SCADA system would then have no ability to adjust to changing conditions; however, except in extreme cases such as peak winter demand conditions, it should be able to maintain deliveries until field personnel arrive and institute manual control. Discussions with natural gas system operators provide a consensus that it would be highly unlikely that the natural gas pipeline system would be shut down immediately if it is recognized that there is problem with the field data.

### **Oil**

If the SCADA system for an oil pipeline is inoperative due to the effects of an EMP event, it is the opinion of a number of former pipeline personnel that operations would have to be shut down. A petroleum pipeline failure can be catastrophic. Leaking oil could contaminate water supplies and cause disastrous fires. Based on their experience, it has been stated that companies that operate any type of complex pipeline system today do not have enough personnel to manually operate the system using on-site operators with telephone communications (which may not be available after an EMP event) to a central control center, due in part to the multiple sites that need to be monitored and controlled during an emergency. Over the past decade, there has been a trend to increase remote control capability while reducing personnel in the oil and natural gas pipeline industry.

U.S. refineries are critically dependent on the computers and integrated circuitry associated with process control, which are vulnerable to EMP effects. Discussions with plant managers and process control engineers at a number of refineries gave a nearly unanimous response that loss of process control would lead to refinery shutdown. A number of refineries stated they maintain an emergency override fail-safe system that institutes a controlled shutdown of the refinery if various SCADA parameters are out of range. However, the very short notice of a process control outage and the emergency shutdown procedure a refinery must undergo significantly increase the potential for equipment damage and lost production.



### Indirect Effects of EMP: Accounting for Infrastructure Interdependencies

Infrastructure interdependency was discussed from a more general perspective in Chapter 1. The petroleum and natural gas infrastructures provide illustrative examples of such interdependencies as illustrated in **figures 5-5** and **5-6**.<sup>7</sup>

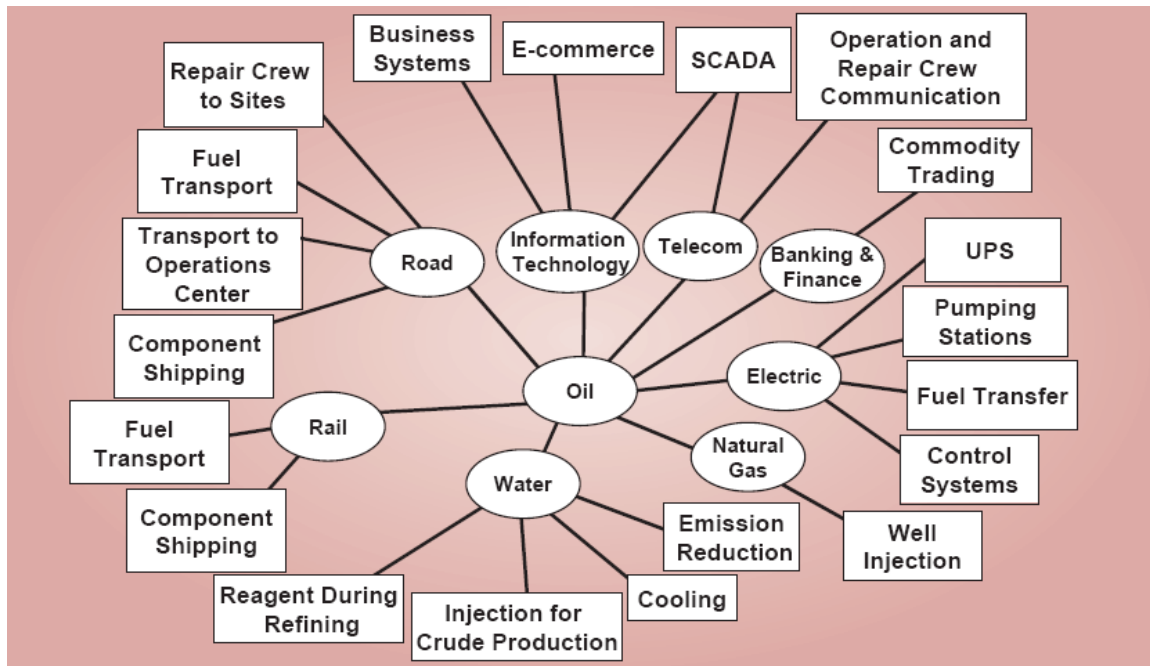


Figure 5-5. Examples of Oil Interdependencies

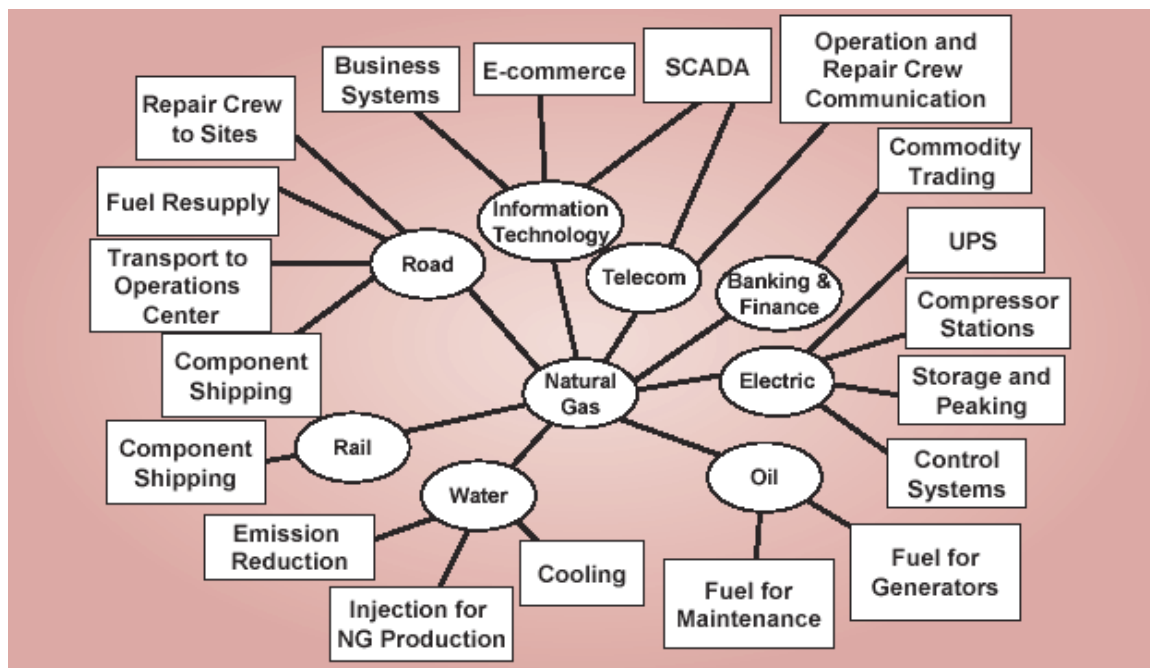


Figure 5-6. Examples of Natural Gas Interdependencies

<sup>7</sup> National Petroleum Council, Securing Oil and Natural Gas Infrastructures in the New Economy. Not all interdependencies are shown.

The petroleum and natural gas infrastructures are critically dependent on the availability of assured electric power from the national grid, as well as all the other critical national infrastructures, including food and emergency services that sustain the personnel manning these infrastructures. In turn, all these infrastructures rely on the availability of fuels provided by the petroleum and natural gas sector.

Petroleum and natural gas systems are heavily dependent on commercial electricity during the entire cycle of production, refining, processing, transport, and delivery to the ultimate consumer. The availability of commercial power is the most important dependency for the domestic oil sector. The natural gas infrastructure depends on electric power to operate lube pumps for compressors, after-cooler fans, electronic control panels, voice and data telecommunication, computers, SCADA communication and controls infrastructure, gas control centers, and other critical components.

U.S. oil and natural gas companies operate a variety of telecommunications systems that are used to provide the internal communications capabilities that are crucial to protecting the safety of life, health, and property. These communications facilities are critical for the day-to-day operations of these companies, as well as for their response to potentially disastrous, life-threatening emergency situations. They are used for the direction of personnel and equipment, the control and synchronization of multiple geophysical acoustical signal sources for oil and gas exploration, and the telemetering of geophysical data. Mobile radio plays a critical role in providing communications for the management of individual wells; pipeline gathering systems; and in the transfer, loading, and delivery of petroleum products to end user consumers. In the event of emergency conditions, communication systems are essential to ensure the safety of personnel, the adjacent population, and the surrounding environment.

Petroleum and natural gas infrastructures are generally well equipped with gas-driven compressors and gas- or diesel-fired pumping facilities and backup generators that would enable the continued flow of natural gas, crude oil, and refined product deliveries for a limited time or that would implement a controlled shutdown following an interruption of electric power supply. There is also a possibility these backup generators may not function after an EMP event if they contain sensitive electronic components such as electronic control units. As one example of interdependency between the fuel and transportation sectors, we note that emergency generators that may keep critical electrical components of the petroleum and natural gas infrastructures running may become inoperative for lack of delivered fuel by a transportation sector short of fuels to run its trucks.

An electric power, water, or transportation disruption of short duration would not necessarily affect the operation of oil and natural gas infrastructure due to backup power and water resources. It is anticipated that crude oil and refined product deliveries could continue to flow for a few days, should these infrastructures be adversely affected. In the short term, natural gas deliveries are facilitated by the combined flexibility afforded by underground storage facilities and by line pack (the volume of gas maintained in the line at pressures above required delivery pressures). But outages of a few days or more can be expected to severely affect all infrastructure operations.

### **Recommendations**

The Federal Government should take the lead in identifying this threat to the oil and gas industry sectors and specify ways to mitigate its potential consequences.

- ◆ The Energy Information Sharing and Analysis Center (ISAC) should, with government funding, expand its mission to address EMP issues relative to the petroleum and natural gas industries. This would include facilitating a government/industry partnership in addressing policy, investment prioritization, and science and technology issues.
- ◆ The Federal Government should review the feasibility of establishing a national inventory of component parts for those items that would be either in great demand or have long lead times, to be made available in a catastrophic event such as an EMP incident.
- ◆ Protect critical components.
  - The oil and natural gas industries should develop resource lists of existing SCADA and process control systems, with prearranged contracts and potential suppliers in the event of an EMP incident.
  - A study should be performed that prioritizes critical facilities of the oil and gas sector for future hardening against EMP effects.
  - Industry should strongly urge its members that have not already done so to install backup control centers to provide operational continuity. Industry should also explore the site location decisions for backup control centers so that adequate geographic separation between the main site and the backup facility is provided to protect against simultaneous damage in the event of a single EMP event.
- ◆ Develop training and exercises.
  - Individual companies should consider engaging in regional response and recovery planning and exercises to deal with disruptions to physical and cyber infrastructures resulting from an EMP event.
  - Emergency response manuals should be revised to include periodically recurring EMP event training for current and future work force.
  - Detailed simulation of the petroleum and natural gas infrastructure on a regional or local basis should be performed to provide a more accurate assessment of the potential impact of EMP-induced damage to these infrastructures.
- ◆ Conduct research.
  - Research and development efforts should stress hardening of SCADA and other digital control systems equipment, both existing and new components, to mitigate the impact of a future EMP event. New standards for oil and gas control systems should be established with the industry to avoid potential damage from EMP effects. These efforts could best be accomplished by the participation of the various industry members, organizations (e.g., American Gas Association [AGA], Interstate Natural Gas Association of America [INGAA], Gas Technology Institute [GTI], American Petroleum Institute [API]), and government agencies.
  - A cost-benefit analysis should be conducted for protecting the commercial petroleum and gas infrastructure against the effects of an EMP. If the costs are estimated to be substantial, the Federal Government should defray a portion of these costs.

## Chapter 6. Transportation Infrastructure

### Introduction

Transportation has played an essential role in our development from scattered settlements to a modern nation. Maritime (i.e., oceanic) shipping sustained the first settlements some five centuries ago and remains the most important avenue for intercontinental commerce today. The 18th century saw the rise of canals in the eastern states, and interest in them lasted through the first decades of the 19th century. Later the railroad supplanted canals in the east and opened the western territories for large-scale economic development and settlement. The 20th century witnessed the advent of the airplane and the automobile, both of which have radically transformed our economy and society. Water, rail, road, and air transportation now bind us together as a nation—economically, socially, and politically.

The criticality of transportation, the impact of potential disruptions, and the need to address vulnerabilities has received national attention. As recognized by the President's National Security Telecommunications Advisory Committee (NSTAC) Information Infrastructure Group Report:<sup>1</sup>

- ◆ The transportation industry is increasingly reliant on information technology (IT) and public information-transporting networks.
- ◆ Although a nationwide disruption of the transportation infrastructure may be unlikely, even a local or regional disruption could have a significant impact. Because of the diversity and redundancy of the United States (U.S.) transportation system, the infrastructure is not at risk of nationwide disruption resulting from information system failure. Nonetheless, a disruption of the transportation information infrastructure on a regional or local scale has potential for widespread economic and national security effects.
- ◆ Marketplace pressures and increasing use of IT make large-scale, multimodal disruptions more likely in the future. As the infrastructure becomes more interconnected and interdependent, the transportation industry will increasingly rely on IT to perform its most basic business functions. As this occurs, it becomes more likely that information system failures could result in large-scale disruptions of multiple modes of the transportation infrastructure.
- ◆ There is a need for a broad-based infrastructure assurance awareness program to assist all modes of transportation.
- ◆ The transportation industry could leverage ongoing research and development initiatives to improve the security of the transportation information infrastructure.
- ◆ There is a need for closer coordination between the transportation industry and other critical infrastructures.

The transportation sector of the economy is often addressed as a single infrastructure, but in reality its various modes provide for several separate, but related, infrastructures. Rail includes the long-haul railroad and commuter rail infrastructures, air includes the commercial and general aviation infrastructures, road includes the automobile and trucking infrastructures, and water includes both the maritime shipping and inland waterway

---

<sup>1</sup> NSTAC Information Infrastructure Group Report, June 1999, <http://www.ncs.gov/nstac/reports/1999/NSTAC22-IIIG.pdf>.

infrastructures.<sup>2</sup> A combination of considerations—importance to the economy, potential for loss of life as a result of an electromagnetic pulse (EMP) attack, and criticality to civilian enterprises—has led us to focus on the long-haul railroad, trucking and automobile, maritime shipping, and commercial aviation infrastructures.

As far as transportation has developed, it is still far from static. The forces driving the continuing evolution of the transportation infrastructures can be understood in terms of the pursuit of competitive advantage, which derives from both lower cost and superior performance. Of particular importance, pressures for cost reduction have led to widespread adoption of just-in-time delivery practices. These practices not only reduce costs associated with maintaining large inventories, but also create strong dependencies on automated tracking of inventories and automatic sorting and loading to achieve efficient and reliable delivery of supplies and equipment. Just-in-time delivery is made possible by the application of technological advances in remote tracking, computer controls, data processing, inventory management, telecommunications, and uninterrupted movement. These technologies are all electronics-based and, hence, potentially vulnerable to EMP.

The imperative to achieve superior performance also has led to greater use of electronics, which has introduced a potential vulnerability to EMP. The automobile provides a familiar example of this phenomenon. Modern automobiles use electronics to increase engine performance, increase fuel efficiency, reduce emissions, increase diagnostic capability, and increase passenger safety and comfort.

To gauge the degree of vulnerability of the long-haul railway, trucking and automobile, maritime shipping, and commercial aviation infrastructures to EMP, the Commission has assessed selected components of these infrastructures that are vital to their operations. Our assessment is based on both data collected from testing conducted under the auspices of the Commission and other available test data that have direct applicability to transportation infrastructure assessment. For critical components of these infrastructures that we were unable to test—notably airplanes, air traffic control centers, locomotives, railroad control centers and signals, and ports—our assessment relies on surveys of equipment and communications links.

*The transportation infrastructures are trending toward increased use of electronics, thereby increasing potential EMP vulnerability.*

### Long-Haul Railroad

Railroads excel at carrying voluminous or heavy freight over long distances. Class I railroad freight<sup>3</sup> in 2003 totaled some 1.8 billion tons originated.<sup>4</sup> The major categories of

<sup>2</sup> Pipelines are sometimes associated with the transportation infrastructure but can be considered more usefully as part of the petroleum and natural gas infrastructures.

<sup>3</sup> The division of railroads into classes based on total operating revenue was a taxonomy defined by the Interstate Commerce Commission in the 1930s. The original threshold for a Class I railroad was \$1 million. In 2006, Class I railroads were those with operating revenues exceeding \$319.3 million. In North America, there are currently seven U.S. railroads that are defined as Class I, with an additional two Canadian railroads that would be considered Class I if U.S. definitions were applied. The old Class II and Class III designators are rarely used today. Instead, the Association of American Railroads speaks of regional railroads operating greater than 350 route-miles or generating more than \$40 million revenue, local line haul carriers with less than 350 route-miles and generating less than \$40 million revenue, and switching and terminal services carriers with highly localized functions, <http://www.railwest.com/railtoday.html>.

<sup>4</sup> “Tons originated” is a common term of art and index in the railroad industry used to track freight traffic volume. It is equal to the tons of traffic shipped by rail. Tons originated rail statistics are available from 1899.



freight carried by railroads, illustrated in **figure 6-1**, include coal, chemicals, farm products, minerals, food products, and a variety of the other goods essential to the operation of our economy.<sup>5</sup>

Coal dominates all other categories of freight, accounting for 44 percent of Class I railroad tonnage in 2003. More than 90 percent of this coal, some 700 million tons, is delivered annually to coal-fired power plants. Power plants that depend on railroad-delivered coal account for more than one-third of our electricity production. Today, these plants typically have only several days' to a month's supply of coal on site. While this reserve provides a useful buffer, under conditions of a prolonged failure of railroads to deliver coal, these plants would simply have to shut down.<sup>6</sup> Electricity production would be affected most in the Midwest, Southeast, and Southwest, regions more heavily dependent on coal-fired power plants.<sup>7</sup>

Railroads have achieved significant gains in efficiency and safety by modernizing and automating their operations. Today, freight railways are controlled and operated from a limited number of centralized control centers. For example, the western U.S. Union Pacific tracks are managed from Omaha, NE, and the Burlington Northern/Santa Fe tracks are managed from Dallas, TX. These centers, as well as operations throughout the rail system, use extensive communication networks for sensing, monitoring, and control. If a railroad control center becomes inoperable or loses communications with the rail network for any reason, all rail traffic in the affected domain will stop until communications are restored or backup procedures are implemented.

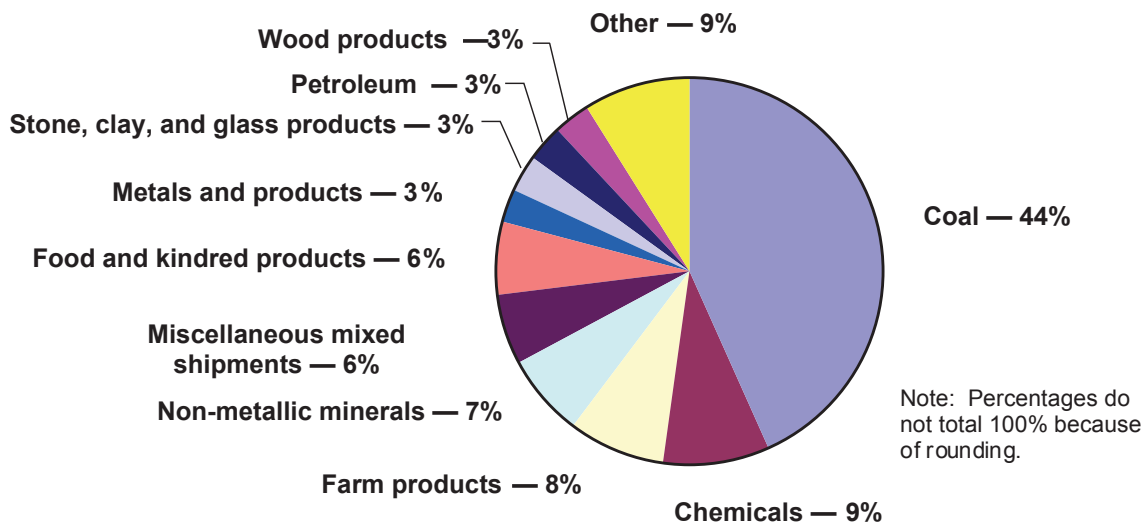


Figure 6-1. 2003 Class I Railroad Tons Originated

### ***EMP Vulnerability of the Long-Haul Railroad Infrastructure***

The principal elements of the railroad infrastructure that we assessed are railroad control centers, railroad signal controls, and locomotives.

<sup>5</sup> Association of American Railroads, <http://www.aar.org>.

<sup>6</sup> Some coal plants also can use natural gas, but this alternative fuel may not be available after an EMP attack. See Chapter 5, Petroleum and Natural Gas Infrastructures.

<sup>7</sup> Association of American Railroads, <http://www.aar.org>.



### *Railroad Control Centers*

We conducted an EMP vulnerability survey of CSX Transportation (CSXT), the railroad subsidiary of the CSX Corporation. CSXT operates the largest rail network in the eastern United States. Like the other major railroad companies, CSXT has centralized its critical control facilities in a single geographical area. The CSXT Jacksonville, FL, railroad control center includes three key nodes, each housed in a separate building—a customer service center, an advanced IT center, and a train dispatch center (**figure 6-2**). These buildings have no specific electromagnetic protection. About 1,200 trains are handled by the CSXT control center in a typical day.

Railroad control center operations rely on modern IT equipment—mainframe and personal computers, servers, routers, local area networks (LAN), tape storage units—some of which are similar to commercial off-the-shelf (COTS) equipment that has been EMP-tested. Based on this similarity, we expect anomalous responses of the IT equipment to begin at EMP field levels of approximately 4 to 8 kV/m. We expect damage to begin at fields of approximately 8 to 16 kV/m.



Figure 6-2. CSXT Train Dispatch Center

The CSXT railroad control center buildings rely on diesel power generators for standby power and central uninterruptible power supply (UPS) systems to provide continuous power to critical loads. Some buildings require chilled water for continuing computer operations. The buildings are interconnected by a fiber-optic ring and telephone lines. None of this equipment has specific EMP protection, and there are no data on the EMP vulnerability of this equipment.

The three railroad control center nodes are almost totally dependent on telephone lines (copper and fiber) for communications and data transfer. If all landlines fail, they still can communicate over a small number of satellite telephones, but data transfers would be severely limited.

Concerns about terrorist attacks and hurricanes have motivated CSXT to make provisions to operate for an extended period without support from the infrastructure. These provisions include diesel generators in case the two independent commercial power feeds should fail, fuel and food stored for 25 to 30 days of operation, beds for 50 people, and on-site wells to provide water.

*Based on our assessment and test results, a weak link in the railroad infrastructure is the railroad signal controls, which can malfunction and slow railroad operations following exposure to EMP fields as low as a few kV/m.*

In addition, all three of the key nodes have remote backup sites, either in Maryland or in the northern Midwest. This geographical dispersion provides some protection from a limited EMP attack. However, these backup sites rely on personnel in the Jacksonville

area for operations at the remote sites, which makes them dependent on the infrastructure for transporting their personnel. It is possible that their personnel could be transported over the CSXT rail system if air and road transportation was interrupted by an EMP attack. They also are dependent on commercial telephone service to transfer the Jacksonville telephone numbers to the alternate sites and to establish the alternate data links.

In the case of EMP-caused outages of the three key facilities and the failure of the backup sites, railroad operations would be severely degraded. Customers could not place shipping orders, data processing would cease, and, most important, train orders could not be generated. Train orders define the makeup of trains, their routes, and their priorities on the track. Trains cannot operate without orders and would revert to fail-safe procedures. The first priority would be to stop the trains. If it were apparent that the outages would last for more than a few hours, efforts would be made to move the trains to the yards. This process could take up to 24 hours.

Once the trains and their crews are secured, plans would be made to resume operations under manual procedures. Implementation of manual procedures could take several days or longer, during which time it would be difficult to operate at more than approximately 10 to 20 percent of normal capacity. Train orders can be issued manually using satellite telephones. The biggest challenge is maintaining communications with trains that are underway. Train yards can communicate with trains by radio. If the trains are within about 20 miles of the yard, the entire communication path is wireless. However, longer-range communications use landlines to repeater stations along the train routes. The repeater station batteries provide only about 24 hours of standby power.

Shipment of critical supplies likely could resume under manual control operations. Transporting food from farms to storage warehouses and from storage warehouses to cities would be a high priority. Trains also deliver chemicals that cities use to purify drinking water and treat waste water. As discussed above, power plants generally have some reserve of coal on hand, but eventually it would become crucial to resume coal shipments to power plants.

### *Railroad Signal Controls*

Railroads use two main types of controls: block controls and local controls. **Figure 6-3** shows a typical block signal control equipment enclosure and antenna. Block controls are used to assure that the next section (block) of track is clear before a train enters it. The main communications from the railroad control centers to the block controls uses a mix of radios and telephones. Block controls have battery backups that can sustain operations for up to 24 hours.

Local control systems manage grade crossings and signal both the train and the road traffic at a crossing. These control systems are designed to operate autonomously. Some modern local control systems have a minimal communications capability that consists of a telephone modem for fault reporting and possible downloading of programs and parameters for the controllers. Local control systems have battery back-up power, which would provide for normal operations from 8 to 48 hours, depending on the volume of train traffic.

**Figure 6-4** shows a typical local grade crossing control shelter and sensor connection. Local control systems have sensors bolted or welded directly to the rails. The resistance of the circuit, closed by the train wheels and axle, is measured and used to predict the train's arrival at the crossing. Modern systems are in shielded steel enclosures that include extensive surge protection.

Similar electronics technologies are used in both road and rail signal controllers. Based on this similarity and previous test experience with these types of electronics, we expect malfunction of both block and local railroad signal controllers, with latching upset beginning at EMP field strengths of approximately 1 kV/m and permanent damage occurring in the 10 to 15 kV/m range.

The major effect of railroad signal control failures will be delayed traffic. For centrally controlled areas of track, if block signals were inoperative, manual block authority would be implemented. Where possible, signal teams would be sent out to manually control failed switches. Crews also would set up portable diesel units to power railroad crossings that had lost power. Railroad crossing generators are on hand for emergencies, such as hurricanes. Repair and recovery times will be on the order of days to weeks. If commercial power is unavailable for periods longer than approximately 24 hours, degraded railroad operations will persist under manual control until batteries or commercial power is restored.



**Figure 6-3. Typical Block Signal Control Equipment Enclosure**



**Figure 6-4. Grade Crossing Shelter and Sensor Connection**

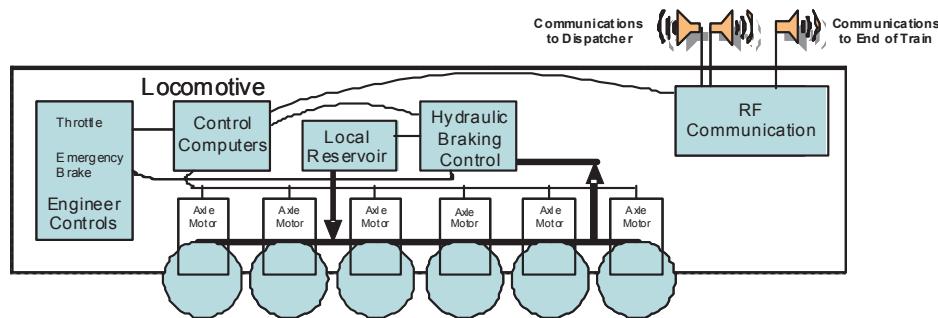
### *Locomotives*

We conducted an assessment of diesel-electric locomotives at the GE Transportation Systems plant (one of two manufacturers of diesel-electric locomotives) in Erie, PA. Our assessment is based on a review of locomotive construction practices, operational procedures, and limited test data. While we do not have direct test data on EMP effects on diesel-electric locomotives, some data are available from a test of a locomotive of different

design that may provide some insight into the robustness of typical locomotive control electronics and subsystems.<sup>8</sup>

Two classes of locomotives were considered—those of the pre-microprocessor era and the more modern locomotives that make extensive use of electronic controls. Approximately 20 percent of the locomotive population is of the older generation; these are rapidly being replaced by the newer models. Electronics are not used to control critical functions in the older locomotives. We consider this generation of locomotives to be immune to EMP effects. While the locomotives themselves are considered immune, loss of communications with central dispatch or within the train requires that the engineer stop the train.

A block diagram showing the critical functions in the more modern locomotives is shown in **figure 6-5**. The major functions are traction (movement) and communications, both of which make extensive use of electronic components and, thus, are potentially vulnerable to EMP. As with older locomotives, the communications include communications to central dispatch and to other parts of the train. If these communications are lost for any reason, the train is required to stop.



**Figure 6-5. Modern Locomotive Functional Block Diagram**

The traction function is totally computer controlled, with the important exception of the engineer's emergency braking system. Three computers are used to control all major subsystems. Malfunction or loss of any of the computers will bring the train to a halt. Restoring operation could require the replacement of computers. Because few spare computers are provisioned, operations could be degraded until new computers are manufactured and installed—a process that could take months.

It is important to note that computer failure or total loss of power in the locomotives could cause loss of electrical control for the brakes. In this case, there is a totally independent, nonelectrical system that the engineer can activate to apply the brakes in both the engine and the cars, thereby halting the train. Therefore, even in the worst case, the engineer can stop the train and prevent train crashes.

Because we did not directly test EMP effects on diesel-electric locomotives, the EMP vulnerability levels can be estimated based only on existing data for computer network response, locomotive construction methods, and the limited data available from the previously referenced test on an electro-mechanical locomotive belonging to the Swiss Fed-

<sup>8</sup> Hansen, R.A., H. Schaer, D. Koenigstein, H. Hoitink, "A Methodology to Assess Exo-NEMP Impact on a Real System—Case Studies," EMC Symposium, Zurich, March 7 to 9, 1989. Reference describes EMP test of electro-mechanical locomotive belonging to Swiss Federal Railways.



eral Railroad.<sup>9</sup> Existing data for computer networks show that effects begin at field levels in the 4 to 8 kV/m range, and damage starts in the 8 to 16 kV/m range. For locomotive applications, the effects thresholds are expected to be somewhat higher because of the large metal locomotive mass and use of shielded cables. Therefore, we expect that effects will likely begin at incident field levels above the 20 to 40 kV/m range.

In summary, we consider the older generation of locomotives to be generally immune to EMP effects. Newer, electronically controlled locomotives are potentially more vulnerable. Based on construction practices, we expect that these vulnerabilities may manifest at EMP levels greater than 20 to 40 kV/m. While vulnerabilities may cause the locomotives to malfunction, fail-safe procedures ensure they can be stopped manually by engineers. Hence, we do not anticipate catastrophic loss of life following EMP exposure. Rather, we anticipate degraded operations, the severity of which depends on the incident EMP field levels. Normal locomotive operations can be restored on time scales from days to weeks or even longer. Restoration time scales could extend to months if computers, for which there are few spares, must be manufactured and replaced.

### **The Automobile and Trucking Infrastructures**

Over the past century, our society and economy have developed in tandem with the automobile and trucking industries. As a consequence, we have become highly dependent on these infrastructures for maintaining our way of life.

Our land-use patterns, in particular, have been enabled by the automobile and trucking infrastructures. Distances between suburban housing developments, shopping centers, schools, and employment centers enforce a high dependence on the automobile. Suburbanites need their cars to get food from the grocery store, go to work, shop, obtain medical care, and myriad other activities of daily life. Rural Americans are just as dependent on automobiles, if not more so. Their needs are similar to those of suburbanites, and travel distances are greater. To the extent that city dwellers rely on available mass transit, they are less dependent on personal automobiles. But mass transit has been largely supplanted by automobiles, except in a few of our largest cities.

As much as automobiles are important to maintaining our way of life, our very lives are dependent on the trucking industry. The heavy concentration of our population in urban and suburban areas has been enabled by the ability to continuously supply food from farms and processing centers far removed. Today, cities typically have a food supply of only several days available on grocery shelves for their customers. Replenishment of that food supply depends on a continuous flow of trucks from food processing centers to food distribution centers to warehouses and to grocery stores and restaurants. If urban food supply flow is substantially interrupted for an extended period of time, hunger and mass evacuation, even starvation and anarchy, could result.

Trucks also deliver other essentials. Fuel delivered to metropolitan areas through pipelines is not accessible to the public until it is distributed by tanker trucks to gas stations. Garbage removal, utility repair operations, fire equipment, and numerous other services

---

<sup>9</sup> The Swiss executed both free-field (up to 25 kV/m) and current-injection (up to 2 kA) tests on a 4.6 MW, 80-ton electro-mechanical locomotive in both power-on and power-off configurations. During the free-field illumination, the test report states that "important analog/digital control electronics, deep inside the PC-boards, was repeatedly burnt out."

are delivered using specially outfitted trucks. Nearly 80 percent of all manufactured goods at some point in the chain from manufacturer to consumer are transported by truck.

The consequences of an EMP attack on the automobile and trucking infrastructures would differ for the first day or so and in the longer term. An EMP attack will certainly immediately disable a portion of the 130 million cars and 90 million trucks in operation in the United States. Vehicles disabled while operating on the road can be expected to cause accidents. With modern traffic patterns, even a very small number of disabled vehicles or accidents can cause debilitating traffic jams. Moreover, failure of electronically based traffic control signals will exacerbate traffic congestion in metropolitan areas. In the aftermath of an EMP attack that occurs during working hours, with a large number of people taking to the road at the same time to try to get home, we can expect extreme traffic congestion. Eventually, however, people will get home and roads will be cleared as disabled cars are towed or pushed to the side of the road.

Our test results show that traffic light controllers will begin to malfunction following exposure to EMP fields as low as a few kV/m, thereby causing traffic congestion. Approximately 10 percent of the vehicles on the road will stop, at least temporarily, thereby possibly triggering accidents, as well as congestion, at field levels above 25 kV/m.

After the initial traffic congestion has subsided, the reconstitution of the automobile and trucking infrastructures will depend primarily on two factors—the availability of fuel and commercial power. Vehicles need fuel and service stations need electricity to power pumps. Few service stations have backup generators. Thus, replenishing the fuel supply and restoring commercial power will pace the return to normal operations. Similarly, restoration of traffic control systems will depend on the availability of commercial power and on the repair of damaged traffic control signals.

### **EMP Vulnerability of the Automobile and Trucking Infrastructures**

We tested the EMP susceptibility of traffic light controllers, automobiles, and trucks.

#### *Traffic Light Controllers*

The road traffic control system is composed of sensors, control, and output systems. **Figure 6-6** shows a typical signalized intersection.



**Figure 6-6. A Typical Signalized Intersection**



Control systems are implemented according to one of several specifications that have evolved over the years. We performed tests of 170E type controllers, in use in approximately 80 percent of signalized intersections. We tested a single controller box populated by multiple electronics cards. In the course of the testing, various cards were damaged and subsequently replaced to continue the testing. Four different types of effects were observed during intersection controller tests:

1. Forced Cycle: At field levels of 1 to 5 kV/m, the light was forced to cycle from green to red without going through yellow. This is a transient effect that recovers automatically after one cycle.
2. Disrupted Cycle: At field levels of 5 to 10 kV/m, the normally programmed cycle times became corrupted and change to a cycle different from that originally programmed. The controller had either been damaged or needed to be manually reset.
3. No Cycle: At 10 to 15 kV/m, the side street lights at an intersection never turned green. The controller had been damaged.
4. Flash Mode: Also at 10 to 15 kV/m, the intersection went into a mode in which the lights in all directions were flashing. This mode can cause large traffic jams because traffic flow is severely reduced in this situation. The controller has either been damaged or needs to be manually reset.

Based on these results, we anticipate that EMP will trigger moderate to severe traffic congestion in metropolitan areas. The traffic congestion may be exacerbated by the panic reactions possibly attendant to an EMP attack. None of the data predict or suggest life-threatening conditions; conflicting green lights did not occur during our tests. All the observed effects would cause less traffic disruption than would a power outage, which results in no working traffic lights.

The highway network's dependency on electrical power was demonstrated during Hurricane Isabel in 2003. Although some critical intersections were equipped with back-up power supplies, they typically were operational only for 24 hours. In many localities, during power outages, law enforcement officers were required to control the critical intersections. As such, these officers were taken away from other activities that they could be serving during emergencies.

Reestablishing normal traffic flow depends on the severity of the EMP-induced faults. Manual resets for all traffic signals in a medium-sized city (population of 500,000) can be accomplished in approximately a day, assuming available personnel.<sup>10</sup> The timeline for repairing damaged traffic controller boxes depends on the availability of spare parts. The timeline for either manual resets or repairs under stressed conditions are unknown.

Major metropolitan areas are establishing traffic operations centers (TOC) as an integral part of their traffic control infrastructure. A city's TOC is responsible for downloading the parameters controlling traffic signal timing and traffic signal coordination. However, a TOC is not a critical node from a traffic control standpoint. If the center were to become inoperable, the immediate effect would be on the city's integrated traffic system; the city would not be able to monitor its roadways, use its variable message signs along priority roadways such as interstates, or produce content for the cable channels or Internet updates that provide the public with information on traffic and highway conditions. The primary long-term effect of a TOC failure would be a gradual drifting of the signal timing synchronization that the center provides to the intersections to which it connects.

---

<sup>10</sup> Conversation with Colorado Springs lead traffic engineer.

### *Automobiles*

The potential EMP vulnerability of automobiles derives from the use of built-in electronics that support multiple automotive functions. Electronic components were first introduced into automobiles in the late 1960s. As time passed and electronics technologies evolved, electronic applications in automobiles proliferated. Modern automobiles have as many as 100 microprocessors that control virtually all functions. While electronic applications have proliferated within automobiles, so too have application standards and electromagnetic interference and electromagnetic compatibility (EMI/EMC) practices. Thus, while it might be expected that increased EMP vulnerability would accompany the proliferated electronics applications, this trend, at least in part, is mitigated by the increased application of EMI/EMC practices.

We tested a sample of 37 cars in an EMP simulation laboratory, with automobile vintages ranging from 1986 through 2002. Automobiles of these vintages include extensive electronics and represent a significant fraction of automobiles on the road today. The testing was conducted by exposing running and nonrunning automobiles to sequentially increasing EMP field intensities. If anomalous response (either temporary or permanent) was observed, the testing of that particular automobile was stopped. If no anomalous response was observed, the testing was continued up to the field intensity limits of the simulation capability (approximately 50 kV/m).

Automobiles were subjected to EMP environments under both engine turned off and engine turned on conditions. No effects were subsequently observed in those automobiles that were not turned on during EMP exposure. The most serious effect observed on running automobiles was that the motors in three cars stopped at field strengths of approximately 30 kV/m or above. In an actual EMP exposure, these vehicles would glide to a stop and require the driver to restart them. Electronics in the dashboard of one automobile were damaged and required repair. Other effects were relatively minor. Twenty-five automobiles exhibited malfunctions that could be considered only a nuisance (e.g., blinking dashboard lights) and did not require driver intervention to correct. Eight of the 37 cars tested did not exhibit any anomalous response.

Based on these test results, we expect few automobile effects at EMP field levels below 25 kV/m. Approximately 10 percent or more of the automobiles exposed to higher field levels may experience serious EMP effects, including engine stall, that require driver intervention to correct. We further expect that at least two out of three automobiles on the road will manifest some nuisance response at these higher field levels. The serious malfunctions could trigger car crashes on U.S. highways; the nuisance malfunctions could exacerbate this condition. The ultimate result of automobile EMP exposure could be triggered crashes that damage many more vehicles than are damaged by the EMP, the consequent loss of life, and multiple injuries.

### *Trucks*

As is the case for automobiles, the potential EMP vulnerability of trucks derives from the trend toward increasing use of electronics. We assessed the EMP vulnerability of trucks using an approach identical to that used for automobiles. Eighteen running and nonrunning trucks were exposed to simulated EMP in a laboratory. The intensity of the EMP fields was increased until either anomalous response was observed or simulator limits were reached. The trucks ranged from gasoline-powered pickup trucks to large diesel-powered tractors. Truck vintages ranged from 1991 to 2003.

Of the trucks that were not running during EMP exposure, none were subsequently affected during our test. Thirteen of the 18 trucks exhibited a response while running. Most seriously, three of the truck motors stopped. Two could be restarted immediately, but one required towing to a garage for repair. The other 10 trucks that responded exhibited relatively minor temporary responses that did not require driver intervention to correct. Five of the 18 trucks tested did not exhibit any anomalous response up to field strengths of approximately 50 kV/m.

Based on these test results, we expect few truck effects at EMP field levels below approximately 12 kV/m. At higher field levels, 70 percent or more of the trucks on the road will manifest some anomalous response following EMP exposure. Approximately 15 percent or more of the trucks will experience engine stall, sometimes with permanent damage that the driver cannot correct.

Similar to the case for automobiles, the EMP impact on trucks could trigger vehicle crashes on U.S. highways. As a result, many more vehicles could be damaged than those damaged directly by EMP exposure.

### **Maritime Shipping**

The key elements of the maritime infrastructure are ocean-going ships and their ports. We did not perform an EMP assessment of ships.

There are more than 100 major public ports in the United States located along the Atlantic, Pacific, Gulf of Mexico, and Great Lakes coasts, as well as in Alaska, Hawaii, Puerto Rico, Guam, and the U.S. Virgin Islands. Deep-draft ports accommodate ocean-going vessels, which move more than 95 percent of U.S. overseas trade by weight and 75 percent by value.<sup>11</sup>

Ports handle a variety of cargo categorized as bulk cargo, including liquid bulk (e.g., petroleum) and dry bulk cargo (e.g., grain); break bulk cargo in barrels, pallets, and other packages; and general cargo in steel containers. Major commodities shipped through U.S. ports include:<sup>12</sup>

- ◆ Crude petroleum and petroleum products—oil and gasoline
- ◆ Chemicals and related products—fertilizer
- ◆ Coal—bituminous, metallurgical, and steam
- ◆ Food and farm products—wheat and wheat flour, corn, soybeans, rice, cotton, and coffee
- ◆ Forest products—lumber and wood chips
- ◆ Iron and steel
- ◆ Soil, sand, gravel, rock, and stone

### **Port Operations**

Our assessment of maritime shipping infrastructure focuses on ports. EMP assessments were conducted for the Port of Baltimore in Maryland and ports in the Hampton Roads, VA, area. The Port of Baltimore assessment was performed at the Seagirt and Dundalk Marine Terminals. The assessment was hosted by the Maryland Port Administration. The Hampton Roads assessment was hosted by the U.S. Coast Guard (USCG) and conducted

---

<sup>11</sup> American Association of Port Authorities, <http://www.aapa-ports.org>.

<sup>12</sup> Ibid.

at their offices in Portsmouth, VA, and at the Norfolk International Terminal (NIT) in Norfolk—one of three terminals in the Hampton Roads area.

Under Coast Guard mandate, the National Vessel Movement Center (NVMC) was established to track notice of arrival information from ships entering all U.S. ports. The NVMC is located in Kearneyville, WV. All cargo ships greater than 300 gross tons must notify the NVMC at least 96 hours prior to their arrival.

For the ports of Baltimore and Hampton Roads, communications between ships and between ship and shore are primarily by way of very high frequency (VHF) radio. All vessels are required to monitor Channel 16 (156.8 MHz). A system of repeaters allows VHF communications 25 miles off shore. Some vessels have satellite communication systems. All vessels are brought into the ports by a pilot who boards the ship in open water.

#### *Hampton Roads Area Port*

NIT, one of the Hampton Roads area facilities, operates much like a bus stop. Ships with 2,000 to 4,000 containers arrive any hour of the day, any day of the week. A few hundred containers may be offloaded and additional containers loaded onboard. Then, after only 4 to 8 hours in port, the ship sails on to its next port. Most of the ships have regular routes. Some ships (15 percent) contain break bulk cargo, which is packaged cargo not in containers. The third type of cargo is bulk (like coal); however, NIT does not handle bulk cargo.

Containers are loaded on and off the vessels using sophisticated cranes designed specifically for the purpose (**figure 6-7**). The containers typically are loaded onto the chassis of yard trucks that shuttle them to storage locations around the port. In some cases “straddle carriers” are used instead of yard trucks.



**Figure 6-7. Container Cranes and Stored Containers**

Cranes are the key element in the operation of the terminal. The criticality of the cranes is underscored by the fact that repair crews are kept on site at NIT at all times. Repairs are required to be made in 15 minutes or less. Cranes have more than 100 computers and sensors in them. Replacement parts for normally anticipated failures are warehoused on site. However, the numbers of spares are not planned in anticipation of an EMP attack.

Each container has a unique identification number. The container number is noted when it is unloaded from a ship. When it is placed in the yard by one of the yard trucks (or straddle carriers), its parking place is sent to the data center in Portsmouth through a handheld wireless computer. All the container location data are mirrored to the data center at NIT and backed up daily. The data centers have UPS and diesel backup power. Per-



sonnel also walk the yard to reconfirm the accuracy and completeness of the container locations. There are typically 30,000 to 40,000 containers stored at NIT.

Eventually, the container is loaded onto a road truck or rail car for shipment to its destination. A container number is logged whenever the container passes through the entrance area. The final checkpoint has radiation detectors to look for radioactive materials that might be moved out of the terminal.

### *Port of Baltimore*

The 275-acre Seagirt Marine Terminal is exclusively a container terminal. On the land side, containers arrive and leave primarily by truck (95 percent), even though the terminal is adjacent to CSX railroad's Intermodal Container Transfer Facility (ICTF). Seagirt has seven active electric cranes for loading and unloading ship containers. Like NIT, the Seagirt cranes rely on commercial power for their operation.

Nearby Dundalk Marine Terminal is more than twice as large (570 acres) and has a mixture of cargo types: passengers on cruise ships, containers, roll-on/roll-off (ro-ro), and break bulk. Dundalk does not process bulk cargo. The terminal has 10 dockside container cranes, which are of various vintages, all older than the Seagirt cranes. The Dundalk dockside cranes all use diesel-powered electric motors.

Dundalk docks on the channel next to Seagirt are used for ro-ro and break bulk cargos. Ro-ro cargos include automobiles and a large assortment of farm and construction equipment.

Both marine terminals use an assortment of diesel- and diesel/electric-powered equipment to move containers around the yard and onto and off of trucks and railroad cars. Diesel-powered top loaders are used to move and stack containers. **Figure 6-8** shows two of the six diesel/electric-powered rubber tire gantries (RTG) at Seagirt. They provide a more efficient method than the top loaders for moving and stacking containers. Unlike the dockside cranes, whose motion is limited by fixed rails, RTGs can be moved and placed strategically around the terminal.



**Figure 6-8. RTG at Seagirt Marine Terminal**

Information about the containers is transmitted to a central computer unit in the Seagirt computer room using wireless handheld Teklogix units (**figure 6-9**). Information about the status and storage location of each container is stored in the database using input from the handheld units. Conversely, the handheld unit operators can download information about any container from the central database. The container tracking systems at Seagirt and Dundalk are highly automated. Their operation is essentially paperless, which places heavy reliance on the integrity of the databases. To enhance reliability, all critical data are mirrored in near-real time to a nearby backup site (about 1 mile away). In addition, backup tapes are generated every evening. Seven days of backups are maintained at the backup site. The computer room uses a Liebert UPS for short-term backup power. Long-term emergency power is provided by a diesel generator. Because the current unit proved



Figure 6-9.  
Handheld  
Wireless Data  
Unit

to be inadequate during a lightning-induced power outage, a new diesel generator is being installed. The new unit also will provide emergency power to critical equipment outside the computer room.

The land side of operations at Seagirt and Dundalk Marine Terminals is primarily concerned with controlling the ingress and egress of container trucks. Entry is regulated by a series of manned consoles overlooking the truck entry area (**figure 6-10**). Trucks pull up to speaker boxes where the driver provides information about the company, vehicle, and business at the terminal. Operators use remote cameras to read license plate numbers and other vehicle identification markings.

The operator enters the information into the database and is issued a routing slip that is printed near the speaker box. The slip looks similar to an airline boarding pass and contains information about the truck and the container with which it is concerned. The driver then proceeds to a manned checkpoint directly below the entry control consoles. Here, Seagirt personnel examine the routing slip and check the driver's identification before allowing the truck to proceed into the terminal to pick up or drop off a container. A similar check is performed when the truck leaves the terminal. All operations are entered into a database, providing real-time information on the status of each truck and its container. There are typically 1,600 truck operations a day at Seagirt.



Figure 6-10. Truck Control Station

### ***EMP Vulnerability of Maritime Shipping***

An EMP event could affect operations in every phase of the transfer of container cargo from ships at sea to the highways and rails of the United States. The ability to provide information on the cargo and crew 96 hours before reaching all ports in the United States could be degraded by EMP-induced failures at the NVMC. Even if the NVMC is not directly impacted by EMP, the ability of ships and their agents to communicate with the NVMC could be affected by a failure in the telephone system.

The USCG, under the authority of the captain of the port, can allow ships into port without a formal notification to the NVMC. The USCG would likely send one of its cut-



ters to contact ships at sea by VHF radio. Its crew might board the ship and escort it to port. The choice of which ships to allow in and which to stop would be at the discretion of the USCG. Depending on the extent of the EMP-affected areas, ships might also be diverted to alternate ports.

Ships approved to enter port still need a pilot to navigate the inner waterways. Pilots use their own boats to reach the ships and use VHF radios for communication. It is unlikely that all the pilot boats and their radios would be damaged by an EMP event. There are always some that are not operating at any given time. Pilots normally rely on satellites for navigation, but they are capable of navigating using charts and buoys.<sup>13</sup>

An EMP event could slow down the arrival of ships to port, but it would not necessarily stop all arrivals. This was the case for the terminals in the Hampton Roads area after September 11, 2001. The terminals remained open, but the USCG was aggressive in boarding and escorting ships to port.

Once container ships are in port, they are dependent on the dockside cranes to load and unload containers. Most of the container cranes in the Hampton Roads area are powered by commercial power; the few remaining diesel-powered cranes are being replaced by electric cranes. All

*Dockside cranes are electrically powered from commercial power with no backup power source; loss of commercial power caused by EMP exposure would halt loading and unloading until electric power service is restored.*

the dockside cranes at Seagirt also are powered by commercial power. The cranes using commercial power have no backup for commercial power. Thus, loading and unloading of containers would stop at these docks until commercial power is restored. The 10 dockside cranes at Dundalk Marine Terminal are diesel/electric and independent of commercial power.

EMP might damage the container cranes. The cranes have myriad electrical components—programmable logic controllers, sensors, and motors. However, given their height, it is likely that they are struck frequently by lightning. While repair crews and replacement parts are kept on site at all times, these parts are unlikely to be sufficient to meet the replacement needs after an EMP attack.

Once containers are removed from a ship, they are placed in the yard in a numbered parking spot or in block storage, where canisters are stacked together like on a ship. Diesel powered yard trucks and straddle carriers are used for this purpose. It is unlikely that all of them would be damaged beyond repair by an EMP event. There are always units that are not operating, which, based on the test data taken on automobiles and trucks, would make them less likely to be damaged.

Equipment not damaged by EMP will be able to operate as long as it has diesel fuel. Typically, a 10-to-20 day supply of fuel is stored at the terminals. They normally rely on commercially powered electric pumps to move fuel out of the storage tanks, but would improvise alternate methods if there was an extended outage of commercial power.

The actual delivery and removal of containers from the ports is dependent on outside trucks and, to a lesser extent, railroads. Diesel/electric RTGs are used to move containers

<sup>13</sup> Many satellites are likely to be unaffected by either EMP or by enhanced space radiation environment produced by a high-altitude burst (see Chapter 10 of this volume), but there may be some degradation as a result of vulnerabilities of receivers or ground stations.

on and off trucks and rail cars. While RTGs are the most efficient method for moving containers, in the event they all failed, it is possible to load and unload containers with diesel-powered top loaders. Even ordinary forklifts could be used in an emergency. Ro-ro operations are less dependent on the operation of terminal equipment. Cranes are not used to unload the equipment—it just rolls down a ramp. Some break bulk cargo ships have their own cranes for dockside operations.

Container-handling equipment is only part of the port operations process. Record keeping is as important. Each container arriving at the port must be tracked until it leaves the port. If the records are lost, reconciling claims of lost containers could have a significant economic impact.

The location of each canister at the Hampton Roads area ports is stored in a database at a data center in Portsmouth. The data are mirrored to the data center at NIT and backed up daily. Both data centers have a UPS and backup generators. They rely on telephone lines to receive data and to communicate with each other.

It is unlikely that both data centers would be so damaged by EMP that they could not operate. They use multiple personal computers from different manufacturers to process the data. The NIT data center, which was visited as part of the assessment, uses Windows<sup>®</sup> software for some applications and Macintosh<sup>®</sup> software for others. This diversity in location, hardware, and software makes it less likely that there will be a total failure of the data processing system.

Even if all data on the container locations were to be lost, it would be possible to regenerate it in a few days. Personnel routinely roam the yard checking the accuracy of the database. They compare the container's unique number with the number of the parking spot. These personnel could reverse the process and regenerate the database.

The arrangement is similar at the Seagirt and Dundalk Marine Terminals. They have a central computer room with multiple servers that support the critical databases. The computer room also contains the base station for the wireless handheld units, various routers, and myriad telephone cables. There is no shielding that would limit EMP coupling to the large number of cables in the room. EMP-induced upsets should be expected and damage is certainly possible.

Critical data are mirrored to another data center about 1 mile away and backed up daily. Both data centers have a UPS and backup generators. The backup generator at Seagirt is inadequate to maintain operations and is being replaced with a more powerful unit that also will provide backup power to other critical equipment, such as the speakers and cameras at the truck gates.

It is unlikely that both of the Baltimore area data centers would be so damaged by EMP that they could not operate. They use multiple personal computers of different generations and from different manufacturers to process the data. The diversity in location and hardware makes it less likely that there will be a total failure of the data processing system. Paper records also would be needed to track the containers entering and leaving both the land and sea sides of the port. The ports could operate at significantly reduced capacity using a paper-based tracking system if necessary. It likely would take several days to implement the process.

Successful recovery from an EMP event will depend greatly on the availability of power and the ability of the USCG and port personnel to evaluate their situation and

---

modify their operations accordingly. The events of September 11, 2001, and the need to survive periodic hurricanes have fostered the type of planning needed to respond to an EMP event. Although EMP was not directly considered, many of the plans for emergency recovery would be helpful after an EMP event.

During the assessment, it was encouraging that people in authority were clearly capable of responding well to unexpected situations. However, their response to an EMP event could improve significantly if they had a better understanding of what to expect.

### Commercial Aviation

Air travel has become ingrained in our way of life. There were 72 U.S.-certified airline carriers at the end of 2002, employing 642,000 pilots, flight attendants, mechanics, and other workers. U.S. airlines carried 560 million domestic passengers during 2001, logging some 700 billion passenger miles. In addition, U.S. airlines all carry freight to some extent. Commercial air freight shipments totaled about 22 billion ton-miles.<sup>14</sup>

The key elements of commercial aviation infrastructure that we assessed are the air traffic control system and the aircraft themselves.

The Federal Aviation Administration (FAA) has the responsibility for operating the U.S. air traffic control system with an emphasis on passenger safety. The FAA rigorously controls commercial air traffic—on the ground at airports (by airport towers), all takeoffs and landings (by Terminal Radar Approach CONTROL—TRACONS), and all en route travel (by air route traffic control centers—ARTCCs). Two essential parts of the FAA air traffic control architecture are (1) command and control through communication among controllers and between controllers and pilots, and (2) navigation aids for following proper routes, terminal approaches, and landing.

Commercial air traffic in U.S. airspace at altitudes up to 70,000 feet is controlled at all times. U.S. airspace is divided into 24 regions, 21 for the contiguous states and one each for Alaska, Hawaii, and Guam. Each region is controlled by an ARTCC. These centers provide en route control for aircraft at altitudes above 17,000 feet, maintaining safe separation between aircraft and routing aircraft around bad weather. Terminal control is provided for aircraft at lower altitudes and on the ground by airport towers.

An ARTCC has an operations room (**figure 6-11**) that consists of rows (banks) of individual controllers. The region controlled by a center is divided into sections. Aircraft are tracked and controlled by individual controllers and handed from controller to controller as the aircraft moves from section to section. Control passes from ARTCC to ARTCC over a dedicated private network telecommunications link that connects a controller from one facility to the next controller at another



Figure 6-11. An ARTCC Operations Room

<sup>14</sup> Bureau of Transportation Statistics.

facility. En route control is acquired and handed off to a terminal controller in a similar manner.

If terminal control is interrupted, en route control takes over. If an en route control center is interrupted, control is turned over to another en route control center. These protocols provide redundant backup capability.

Radars are used to acquire and track aircraft in support of air traffic control centers. Generally, multiple radars will track an aircraft. Computers in air traffic control centers process radar information to form mosaic sectional displays and pass aircraft tracking information from center to center and across sections at a control center. Visualization is with a cathode ray tube (CRT) screen; paper printouts are also provided and used as a backup. Given a large number of radars with overlapping coverage, failure of a single radar will not adversely affect commercial air operations. Simultaneous failure of multiple radars, as could happen in an EMP attack, could shutdown all air traffic in the affected region, possibly nationwide.

The commercial aircraft in use are primarily jet-powered aircraft constructed by Boeing in the United States, and Airbus in Europe. In addition, there are various manufacturers of smaller commuter aircraft.

More than any other transportation infrastructure, the commercial aviation infrastructure is based on electronics. Everything from fly-by-wire aircraft flight control systems to navigation, communications, engine sensors and controls, and essential ground-based operations depends on microprocessor computer control.

Although a shutdown or curtailment of commercial aviation would have a severe, perhaps crippling, impact on the airline industry itself, the consequences for critical infrastructures would be less serious. Few vital economic activities are highly dependent on the unique advantage—speed—that commercial air transport has over the various modes of land transport.

### ***EMP Vulnerability of the Commercial Aviation Infrastructure***

#### ***Aircraft***

Our commercial aircraft EMP assessment was conducted based on results of a meeting and subsequent discussions with Boeing electromagnetics effects (EME) staff. This staff is responsible for assuring that Boeing commercial aircraft can operate following exposure to nonhostile electromagnetic (EM) environments. Specifically, we assessed the amount of EMP protection that might be afforded by protection against lightning and high-intensity radiated fields (HIRF). Moreover, our assessment focused on safety of flight and the capability to land a plane after EMP exposure. We did not address continuation of normal flight operations, because we expect that all aircraft will be directed to land immediately on notification of an EMP attack.

Boeing maintains a strict engineering protocol for assuring their commercial aircraft are protected against nonhostile EM environments. This protocol includes qualification testing that is a function of flight-critical electronics categories, application of immunity standards to electronics boxes (sometimes referred to as line-replaceable units [LRU]), and hardening practices tailored to specific requirements.

*EME Qualification Practices for Safety-of-Flight Electronics.* Boeing assigns electronics equipment to categories to differentiate the impact of loss of function. The highest category is reserved for electronics boxes, the failure of which would be considered catastrophic, and could lead to potential loss of the aircraft. Because our assessment focused on safety of flight, this is the most important category for EMP effects.

For this category of electronic subsystems, EME qualification is performed by a combination of low-level system tests and electronics box immunity tests (see next section). The purpose of the system-level tests is to estimate the intensity of the electromagnetic stresses coupled to the electronics box interfaces (connectors). For lightning (the EM environment most similar to EMP), the box immunity tests are then used to demonstrate that the electronics immunity levels are at least a factor of two higher than the coupled stresses. If this margin is not achieved, Boeing adjusts the protection tactics until this requirement is met. For lower-criticality electronic systems, only the box immunity tests are conducted, and there is no explicit relationship to the coupled stress required.

◆  
*Although commercial aircraft have proven EM protection against naturally occurring EM environments, we cannot confirm safety of flight following EMP exposure. Moreover, if the complex air traffic control system is damaged by EMP, restoration of full services could take months or longer.*

There has been significant evolution in the use of electronics in commercial aircraft. For aircraft designs prior to the 777, a direct mechanical/hydraulic link to the control surfaces was maintained, thereby minimizing electronics criticality for safety-of-flight applications. This observation would mitigate in favor of inherent EMP immunity for the nonelectronic subsystems. However, depending on aircraft, there are still some flight-critical functions performed by electronics, for which EMP immunity is not known. Therefore, even for pre-777 designs, there are insufficient data to confirm EMP immunity. Additional testing (limited to flight-critical electronics) is required to confirm EMP immunity. This testing should include low-level system testing to estimate EMP stresses at electronics interfaces and the corresponding electronics immunity testing. The recommended approach is essentially an extension of the existing lightning protocol to provide coverage for the EMP environment.

Boeing considers the 777 to be their first fly-by-wire design, incorporating more flight-critical electronics than used in earlier designs. Therefore, the newer designs may be more prone to EMP safety-of-flight impact. This potential is significantly mitigated by judicious use of redundancy for flight-critical subsystems. For example, while the flight-control systems use electrical signals rather than mechanical wires for control surface instructions, the primary digital controls are backed up by analog signals. Moreover, significant redundancy (up to four levels) is built into each flight-control subsystem. Therefore, the possible EMP susceptibility is offset significantly by careful, redundant design. Nonetheless, the qualification protocols do not provide adequate coverage for anticipated EMP responses. Therefore, as is the case for the earlier designs, additional testing is required to confirm EMP immunity. This testing should address both the EMP stresses at electronics interfaces and the corresponding immunity testing. Because there is more application of electronics in the newer designs, more extensive testing will be required than for the earlier designs.



*EME Immunity Testing Standards.* The industry standard for electronics immunity testing for commercial aircraft is RTCA/DO-160D.<sup>15</sup> Boeing uses an internal standard that flows down from RTCA/DO-160D but is tailored to the company's technical practices. For lightning, damped sinusoid immunity testing at center frequencies of 1 and 10 MHz is required. Other EMP aircraft testing has shown that EMP response tends to be at higher frequencies, generally in the 10 to 100 MHz range. In addition, conducted susceptibility HIRF testing is required for frequencies covering and extending far beyond the EMP range. However, the test amplitudes are lower than might be expected for EMP. Therefore, EMP survivability cannot be directly inferred from commercial aircraft lightning and HIRF immunity testing standards.

*EME Hardening Practices.* EME hardening in Boeing aircraft is achieved using a combination of tactics-stress reduction (e.g., use of shielded electrical cables), redundancy of flight-critical systems (depending on the system, up to four channels of redundancy are applied), and software error detection/correction algorithms for digital data processing. The combination of these tactics is adjusted to match the specific requirements of different electronic subsystems. In addition, hardening measures may be applied to electronic boxes to increase immunity, if required, to meet the Boeing specifications that flow down from DO-160D.

In summary, the Boeing engineering approach for protection and qualification against nonhostile electromagnetic environments is well established, and it is demonstrated by experience to be sufficient for the EM environments to which the aircraft are exposed during normal operations. While these procedures may provide significant protection in the event of an EMP attack, this position cannot be confirmed based on the existing qualification test protocols and immunity standards. This conclusion is applicable to all commercial aircraft currently in service, including the earlier designs. However, it is particularly emphasized for the newer, fly-by-wire designs that, by virtue of more reliance on digital electronics, may be more prone to EMP effects.

#### *Air Traffic Control*

We conducted an EMP vulnerability assessment of air traffic control by discussions with FAA engineers and former air traffic controllers and by visits to an FAA facility in Oklahoma City and the ARTCC in Longmont, CO. Moreover, because computer networks are integral parts of the air traffic control system, existing EMP test data on similar COTS electronics is applicable. Our testing did not include the FAA's private telecommunications network links connecting the ARTCCs, such as the FAA Leased Interfacility National Air Space Communications System (LINCS) and more recently the FAA Telecommunications Infrastructure (FTI) Program.<sup>16</sup> These FAA critical telecommunications

<sup>15</sup> RTCA, Inc., is a not-for-profit corporation that develops recommendations regarding communications, navigation, surveillance, and air traffic management system issues.

<sup>16</sup> The FAA LINCS is a highly diverse private network constructed to meet specific requirements of a customer with critical mission requirements. The FAA LINCS is the most available private line network in the world with an off-backbone availability requirement of 99.8 percent. More than 21,000 circuits serve the entire network. More than 200 circuits form the LINCS backbone and satisfy diversity requirements of 99.999 percent availability. Despite natural disasters, major failures of public infrastructures, and the 2001 terrorist attacks, the FAA LINCS survived as designed, keeping the line of communication open between air traffic controllers and airplanes. In July 2002, the FAA initiated a substantial modernization of its telecommunications networks to meet its growing operational and mission support requirements and to provide enhanced security features. The new FTI Program is an integrated suite of products, services, and business practices that provide a common infrastructure supporting the National Airspace System (NAS) requirements for voice, data, and video services; improve visibility into network operations, service delivery status, and cost of services; and integrate new technologies as soon as they emerge. Reference: NSTAC Financial Services Task Force Report on Network Resilience, [http://www.ncs.gov/nstac/nstac\\_publications.html](http://www.ncs.gov/nstac/nstac_publications.html).



networks and services are supported by a number of National Security and Emergency Preparedness (NS/EP) programs available from the Department of Homeland Security (DHS) National Communications System (NCS).<sup>17</sup>

The main function of ARTCCs is to control air traffic in surrounding regions. Regions are divided into sections and aircraft are monitored from section to section before being handed off to another ARTCC or to an airport approach control center. The process is highly computerized with quadruple computer redundancy and redundant power and internal communication systems.

The ARTCCs are composed, in part, of computer networks based on commercial components. Similar components have been EMP tested and have manifested latching upsets (requiring manual intervention to restore function) beginning in the 4 kV/m peak field range. Permanent damage has been observed in the 8 kV/m range but is more prevalent above 15 kV/m. Based on similarity, it is anticipated that ARTCCs will begin to manifest loss of function following EMP exposure to peak fields as low as 4 kV/m; but functions will not be seriously degraded unless exposed to peak fields in excess of 15 kV/m.

A large number of radars have overlapping coverage. Failure of a single radar will not significantly impact air traffic control capability. Simultaneous failure of multiple radars, as could happen in an EMP attack, could shutdown all air traffic control in the affected region, and possibly nationwide, thereby making it more difficult to assure safe landings. In this case, emphasis for safe landings would shift to aircraft crew and airport towers.

Power to all critical components of the FAA system is backed by fuel generator power, and in some instances, uninterrupted through temporary use of large UPSs. Visual flight operations will be in the forefront for collision avoidance and landing. Many aircraft will land at airports other than originally intended, as was the case after the 9/11 terrorist attacks. Significant challenges arise for safe landing in conditions of low visibility in the absence of navigation and landing aids at night and during adverse weather.

There are redundant radio communications with aircraft and redundant telephone and microwave communications between air traffic control regions and airport towers. If communications are lost, responsibility for safe landings will revert solely to the aircraft crews.

If the FAA air traffic control system is damaged by exposure to EMP environments, its reconstitution would take time. The FAA does not have sufficient staff or spare equipment to do a mass rapid repair of essential equipment. The FAA collection of radar, communication, navigation, and weather instruments spans 40 years. It includes components from multiple vendors that are connected using a variety of wire, wireless, and fiber links. Some equipment has lightning and electromagnetic interference protection. Accordingly, configuration control is difficult. It would take days to a month or more to bring various components of the control system back online, starting with communications, followed with navigation aids. As the control system rebuilds, there is likely to be significant reduction in air traffic, with constraints to increase intervals for departures, landings, and spacing of aircraft en route. Moreover, the capability to restore the air traffic control system is dependent on availability of services from other infrastructures. In the event these services are compromised by an EMP attack, the air traffic control restoration times will be extended.

---

<sup>17</sup> Telecommunications Service Priority (TSP), <http://tsp.ncs.gov>.

## Recommendations

Specific actions for each transportation infrastructure follow.

### ***Railroads***

Railroad operations are designed to continue under stressed conditions. Backup power and provisioning is provided for operations to continue for days or even weeks at reduced capacity. However, some existing emergency procedures, such as transferring operations to backup sites, rely on significant warning time, such as may be received in a weather forecast before a hurricane. An EMP attack may occur without warning, thereby compromising the viability of available emergency procedures. Our recommendations are directed toward mitigating this and other potential weaknesses. DHS should:

- ◆ Heighten railroad officials' awareness of the possibility of EMP attack, occurring without warning, that would produce wide-area, long-term disruption and damage to electronic systems.
- ◆ Perform a test-based EMP assessment of railroad traffic control centers. Develop and implement an EMP survivability plan that minimizes the potential for adverse long-term EMP effects. The emphasis of this effort should be on electronic control and telecommunication systems.
- ◆ Perform an EMP vulnerability assessment of current vintage railroad engines.
- ◆ Develop and implement an EMP survivability plan, if needed.

### ***Trucking and Automobiles***

Emphasizing prevention and emergency clearing of traffic congestion, DHS should coordinate a government and private sector program to:

- ◆ Initiate an outreach program to educate state and local authorities and traffic engineers on EMP effects and the expectation of traffic signal malfunctions, vehicle disruption and damage, and consequent traffic congestion.
- ◆ Work with municipalities to formulate recovery plans, including emergency clearing of traffic congestion and provisioning spare controller cards that could be used to repair controller boxes.
- ◆ Sponsor the development of economical protection modules—preliminary results for which are already available from Commission-sponsored research—that could be retrofitted into existing traffic signal controller boxes and installed in new controller boxes during manufacturing.

### ***Maritime Shipping***

The essential port operations to be safeguarded are ship traffic control, cargo loading and unloading, and cargo storage and movement (incoming and outgoing). Ship traffic control is provided by the Coast Guard, which has robust backup procedures in place. Cargo storage and movement is covered by other transportation infrastructure recommendations. Therefore, focusing on cargo operations in this area, DHS should coordinate a government and private sector program to:

- ◆ Heighten port officials' awareness of the wide geographic coverage of EMP fields, the risk caused by loss of commercial power for protracted time intervals, and the need to evaluate the practicality of providing emergency generators for at least some portion of port and cargo operations.
- ◆ Assess the vulnerability of electric-powered loading and unloading equipment.

- ◆ Review the electromagnetic protection already in place for lightning and require augmentation of this protection to provide significant EMP robustness.
- ◆ Coordinate findings with the real-time repair crews to ensure they are aware of the potential for EMP damage, and, based on the assessment results, recommend spares provisions so that repairs can be made in a timely manner.
- ◆ Assess port data centers for the potential of loss of data in electronic media.
- ◆ Provide useful measures of protection against EMP causing loss of function data.
- ◆ Provide protected off-line spare parts and computers sufficient for minimum essential operations.
- ◆ Provide survivable radio and satellite communication capabilities for the Coast Guard and the nation's ports.

***Commercial Aviation***

In priority order, commercial aviation must be assured that airplanes caught in the air during an EMP attack can land safely, that critical recovery assets are protected, and that contingency plans for an extended no-fly period are developed. Thus, DHS, working with the Department of Transportation, should:

- ◆ Coordinate a government program in cooperation with the FAA to perform an operational assessment of the air traffic control system to identify and provide the minimal essential capabilities necessary to return the air traffic control capability to at least a basic level of service after an EMP attack.
- ◆ Based on the results of this operational assessment, develop tactics for protection, operational workarounds, spares provisioning, and repairs to return to a minimum-essential service level.

***All Transportation Sectors***

- ◆ DHS should incorporate EMP effects assessment in existing risk assessment protocols.

## Chapter 7. Food Infrastructure

### Introduction

A high-altitude electromagnetic pulse (EMP) attack can damage or disrupt the infrastructure that supplies food to the population of the United States. Food is vital for individual health and welfare and the functioning of the economy.

### Dependence of Food on Other Infrastructures

The food infrastructure depends critically for its operation on electricity and on other infrastructures that rely on electricity. An EMP attack could disrupt, damage, or destroy these systems, which are necessary in making, processing, and distributing food.

Agriculture for growing all major crops requires large quantities of water, usually supplied through irrigation or other artificial means using electric pumps, valves, and other machinery to draw or redirect water from aquifers, aqueducts, and reservoirs. Tractors and farm equipment for plowing, planting, tending, and harvesting crops have electronic ignition systems and other electronic components. Farm machinery runs on gasoline and petroleum products supplied by pipelines, pumps, and transportation systems that run on electricity or that depend on electronic components. Fertilizers and insecticides that make possible high yields from croplands are manufactured and applied through means containing various electronic components. Egg farms and poultry farms typically sustain dense populations in carefully controlled environments using automated feeding, watering, and air conditioning systems. Dairy farms rely heavily on electrically powered equipment for milking cattle and for making other dairy products. These are just a few examples of how modern food production depends on electrical equipment and the electric power grid, which are both potentially vulnerable to EMP.

Food processing also requires electricity. Cleaning, sorting, packaging, and canning of all kinds of agricultural products are performed by electrically powered machinery. Butchering, cleaning, and packaging of poultry, pork, beef, fish, and other meat products also are typically automated operations, done on electrically driven processing lines. An EMP attack could render inoperable the electric equipment and automated systems that are ubiquitous and indispensable to the modern food processing industry.

Food distribution also depends heavily on electricity. Vast quantities of vegetables, fruits, and meats are stored in warehouses, where they are preserved by refrigeration systems, ready for distribution to supermarkets. Refrigerated trucks and trains are the main means of moving perishable foods to market; therefore, food distribution also has a critical dependence on the infrastructure for ground transportation. Ground transportation relies on the electric grid that powers electric trains; runs pipelines and pumping stations for gasoline; and powers signal lights, street lights, switching tracks, and other electronic equipment for regulating traffic on roads and rails.

Because supermarkets typically carry only enough food to supply local populations for 1 to 3 days and need to be resupplied continually from regional warehouses, transportation and distribution of food to supermarkets may be the weakest link in the food infrastructure in the event of an EMP attack. The trend toward modernization of supermarkets may exacerbate this problem by deliberately reducing the amount of food stored in supermarkets and regional warehouses in favor of a new just-in-time food distribution system. The new system relies on electronic databases to keep track of supermarket inventories so that they can be replaced with fresh foods exactly when needed, greatly reducing the need for large stocks of warehoused foods.

---

The electric power grid, on which the food infrastructure depends, has been component-tested and evaluated against EMP and is known to be vulnerable. Moreover, power grid blackouts induced by storms and mechanical failures on numerous occasions have caused massive failure of supermarket refrigeration systems and impeded transportation and distribution of food, resulting in spoilage of all perishable foods and causing food shortages lasting days or sometimes weeks. These storm- and accident-induced blackouts of the power grid are not likely to have consequences for the food infrastructure as severe or as geographically widespread as an EMP attack would.

In the face of some natural disasters like Hurricane Andrew in 1992, federal, state, and local emergency services combined have sometimes been hard pressed to provide the endangered population with food. Fortunately, there are few known instances of actual food starvation fatalities in the United States. In such localized emergencies as Hurricane Andrew, neighboring areas of the disaster area are usually able to provide needed emergency services (e.g., food, water, fire, and medical) in a timely fashion.

In the case of Hurricane Andrew, for example, although the area of the damage was relatively small, the level of damage was extraordinary and many people were affected. Consequently, emergency services were brought in, not just from neighboring states, but from many distant states. For example, electric transformers were brought in from other states to help rebuild the local power grid. The net result was a nationwide shortage of transformers for 1 year until replacements could be procured from overseas suppliers, who needed 6 months to build new transformers.

Hurricane Katrina, one of the greatest natural disasters ever to strike the United States, afflicted a much larger area than Andrew. Consequently, the ability to provide food and other emergency aid was a much greater challenge. The area disrupted by Hurricane Katrina is comparable to what can be expected from a small EMP attack.

Recent federal efforts to better protect the food infrastructure from terrorist attack tend to focus on preventing small-scale disruption of the food infrastructure, such as would result from terrorists poisoning some portion of the food supply. Yet an EMP attack potentially could disrupt or collapse the food infrastructure over a large region encompassing many cities for a protracted period of weeks, months, or even longer. Widespread damage of the infrastructures would impede the ability of undamaged fringe areas to aid in recovery. Therefore, it is highly possible that the recovery time would be very slow and the amount of human suffering great, including loss of life.

### **Making, Processing, and Distributing Food**

The United States is a food superpower. It leads the world in production of the 10 major crops, nine of which are food sources: corn, soybeans, wheat, upland cotton, sorghum, barley, oats, rice, sunflowers, and peanuts. The United States is also a world leader in the production of meats, poultry, and fish. Of the world's 183 nations, only a few are net exporters of grain. The United States, Canada, Australia, and Argentina supply over 80 percent of the net cereal grains exported worldwide—the United States alone providing more than half.

These U.S. exports go far toward alleviating hunger and preserving political stability in many nations that lack the resources to feed their own populations. While most Americans tend to take for granted the quantity and high quality of food available to them on a daily basis, most other countries of the world regard the United States' food infrastructure as an enviable economic miracle.



In contrast to the United States, many of the world's nations struggle to meet the food demands of their populations, even though in some cases those populations are living near or below a subsistence level. Most of the world's 183 nations, to some degree, are dependent on food imports. Even among the advanced nations, the United States is exceptional for the quantity and quality of its food production.

U.S. consumers are supplied largely from domestically produced food. In 2002, according to data from the U.S. Department of Agriculture (USDA), some 2.1 million U.S. farms sold about \$192 billion in crops and livestock. U.S. farms have 455 million acres under cultivation for crop production. Another 580 million acres in the United States are pasture and range land that support raising livestock.

Raw agricultural commodities are converted to intermediate foodstuffs and edible foods by some 29,000 processing plants located throughout the United States, according to the Census of Manufacturers. These plants employ about 1.7 million workers, which is approximately 10 percent of all U.S. manufacturing employment and just over 1 percent of all U.S. employment. Most plants are small, but larger establishments account for the major portion of shipments. The 20 largest firms in food manufacturing account for about 35 percent of shipments, while in beverage manufacturing, the 20 largest firms account for 66 percent of shipments. The largest 50 firms account for 51 percent of food shipments and 74 percent of beverage shipments.

Food is supplied to consumers by approximately 225,000 food stores, as well as by farmers markets and pick-your-own farms. Away-from-home food service is provided by approximately 850,000 establishments, including restaurants, cafeterias, fast food outlets, caterers, and others.

To illustrate how the U.S. food infrastructure works in making, processing, and distributing food from farm to market, here is a concrete example:

Washington State is the foremost apple producer in the United States, with more than \$850 million in annual sales and 225,000 acres of orchards, mostly in the Cascade Mountains. A major supermarket chain contracts through a cooperative of medium-sized apple growers in the Spokane area to grow apples.

In the course of the growing season, the Spokane apple farmers use a wide array of farm machinery to tend their trees and to apply fertilizers and pesticides. During the harvest season, Washington farmers employ 35,000 to 45,000 pickers to harvest their apple crops. Hand-picked apples are loaded onto flatbed trucks and shipped to processing firms belonging to or under contract with the chain. Apples are processed on an electrically driven assembly line that uses a variety of electromechanical devices to clean fruit of dirt and pesticide residue, sort and grade apples according to size and quality, wax the fruit, and package it into 40-pound cartons.

If the apples are not to be sent to market immediately, they can be stored for up to 8 months in giant refrigerators. The chain arranges for a shipment of apples to its Maryland distribution center, located in Upper Marlboro, which services its stores in the Washington, D.C., area. A trucking company is contracted for the 4-to-5 day shipment of apples to the East Coast using a refrigerated truck. The apples are offloaded at the Upper Marlboro regional distribution center, which makes daily deliveries to the chain's stores. A refrigerated truck delivers apples to a Washington, D.C., supermarket. Local residents purchase the apples.



This example of how the food infrastructure works for apples from grower to consumer generally is the same for most foods, with differences in detail. One important difference is that apples, compared to many other crops, are among those most dependent on manual labor and least dependent on machinery. Yet, clearly the food infrastructure, even for the apple, depends heavily on assembly lines, mechanical sorters and cleaners, refrigerators, and vehicles that, directly or indirectly, cannot operate without electricity.

### **Vulnerability to EMP**

An EMP attack could damage or destroy some fraction of the myriad electronic systems, ubiquitous throughout the food infrastructure, that are essential to making, processing, and distributing food. Growing crops and raising livestock require vast quantities of water delivered by a water infrastructure that is largely electrically powered. Tractors, planters, harvesters, and other farm equipment are fueled by petroleum products supplied by pipelines, pumps, and transportation systems that run on electricity. Fertilizers, insecticides, and feeds that make possible high yields from crops and livestock are manufactured by plants requiring electric power.

Food processing—cleaning, sorting, packaging, and canning of all kinds of agricultural and meat products—is typically an automated operation, performed on assembly lines by electrically powered machinery.

Food distribution also depends on electricity. Refrigerated warehouses make possible the long-term storage of vast quantities of vegetables, fruits, and meats. Road and rail transportation depend on the electric grid that powers electric trains, runs pipelines and gas pumps, and powers the apparatus for regulating traffic on roads and rails.

Because the United States is a food superpower with relatively few farmers, technology is no longer merely a convenience—it is indispensable to the farmers who must feed the nation's population and much of the rest of the world.

In 1900, 39 percent of the U.S. population (about 30 million people) lived on farms; today that percentage has plummeted to less than 2 percent (only about 4.5 million people). The United States no longer has a large labor force skilled in farming that could be mobilized in an emergency. The transformation of the United States from a nation of farmers to a nation in which less than 2 percent of the population is able to feed the other 98 percent is made possible only by technology. Crippling that technology would be injurious to the food infrastructure with its security depending on the characteristics of an EMP attack.

The dependency of the U.S. food infrastructure on technology is much greater than implied by the reduction in the percentage of farmers from 39 percent in 1900 to less than 2 percent of the population today. Since 1900, the number of acres under cultivation in the United States has increased by only 6 percent, yet the U.S. population has grown from about 76 million people in 1900 to 300 million today. In order for a considerably reduced number of U.S. farmers to feed a U.S. national population that has grown roughly four-fold from approximately the same acreage that was under cultivation in 1900, the productivity of the modern U.S. farmer has had to increase by more than 50-fold. Technology, in the form of machines, modern fertilizers and pesticides, and high-yield crops and feeds, is the key to this revolution in food production. An attack that neutralized farming technology would depress U.S. food production.

The food processing industry is an obvious technological chokepoint in the U.S. food infrastructure. Food processing of vegetables, fruits, and all kind of meats is a highly automated, assembly-line operation, largely driven by electric power. An EMP attack that damages this machinery or blacks out the power grid would stop food processing. The work force in the food processing industry is sized and trained to run a largely automated system. In the event of an attack that stops the machines from running, personnel would not be sufficiently numerous or knowledgeable to process food the old-fashioned way, by hand. Depending on climate, most foods that are not refrigerated would begin to spoil in a few hours or days.

Finally, the distribution system is probably the most vulnerable technological chokepoint in the U.S. food infrastructure. Supermarkets typically carry only enough food to provision the local population for 1 to 3 days. Supermarkets replenish their stocks virtually on a daily basis from regional warehouses, which usually carry enough food to supply a multicounty area for about 1 month.

Regional warehouses are probably the United States' best near-term defense against a food shortage because of the enormous quantities of foodstuffs stored there. For example, one typical warehouse in New York City daily receives deliveries of food from more than 20 tractor trailers and redistributes to market more than 480,000 pounds of food. The warehouse is larger than several football fields, occupying more than 100,000 square feet. Packaged, canned, and fresh foods are stored in palletized stacks 35 feet high. Enormous refrigerators preserve vegetables, fruits, and meats and the entire facility is temperature controlled.

However, regional warehouses potentially are vulnerable to an attack that collapses the power grid and causes refrigeration and temperature controls to fail. Moreover, the large quantities of food kept in regional warehouses will do little to alleviate a crisis if it cannot be distributed to the population promptly. Distribution depends largely on trucks and a functioning transportation system. Yet storm-induced blackouts have caused widespread failure of commercial refrigeration systems and massive food spoilage.

Trends in the grocery industry toward just-in-time distribution may reduce reliance on regional warehouses and increase the vulnerability of the food infrastructure to EMP attack. Just-in-time distribution, now being adopted by some supermarket chains in California, Pennsylvania, and New Hampshire, uses automated databases and computer systems to track supermarket inventories in real time and promptly replenish food inventories, as needed, from even larger, but fewer, regional warehouses and directly from food manufacturers.

The new system promises to supply customers with fresher foods and to greatly reduce industry's reliance on large inventories of stockpiled foods at regional warehouses. As just-in-time distribution becomes the industry norm, in the event of an EMP attack, heavier reliance on computers and databases may make it easier to disrupt the management of food distribution, while decreased reliance on regional warehouses could greatly reduce the amount of food available for distribution in an emergency.

*Pulse-current injection and free-field illumination testing on a limited number of refrigerators and freezers indicate that some units will fail from low to moderate EMP levels. This testing indicates that substantial numbers of people would have to survive without benefit of refrigerated foods for an extended period, until repairs or replacement refrigerators and freezers could be obtained. Massive food spoilage at stores and regional warehouses is implied.*

### **Consequences of Food Infrastructure Failure**

An EMP attack that disrupts the food infrastructure could pose a threat to life, industrial activity, and social order. Absolute deprivation of food, on average, will greatly diminish a person's capacity for physical work within a few days. After 4 to 5 days without food, the average person will suffer from impaired judgment and have difficulty performing simple intellectual tasks. After 2 weeks without food, the average person will be virtually incapacitated. Death typically results after 1 or 2 months without food.

This timeline would not start until food stockpiles in stores and homes were depleted. Many people have several days to weeks of food stored in their homes. For example, in 1996 when a snowstorm in the Washington, D.C., area virtually paralyzed the food infrastructure for a week, the general population was forced to live off of private food larders and had sufficient stores to see them through the emergency. However, a significant number of people, those with little or no home food supply, would have to begin looking for food immediately.

Historically, even the United States' vast agricultural wealth has not always been enough to protect its people from the effects of nature and bad economic decisions. Millions of Americans knew hunger as a consequence of a drought that caused the dust bowl years (1935 to 1938) in the Western and Central Plains breadbasket, as well as by the Wall Street crash of 1929 and the Great Depression. Even today, according to the USDA, 33.6 million Americans, almost 12 percent of the national population, live in "food-insecure households." Food-insecure households, as defined by the USDA, are households that are uncertain of having or are unable to acquire enough food to meet the nutritional needs of all their members because they have insufficient money or other resources.

A natural disaster or deliberate attack that makes food less available, or more expensive, would place at least America's poor, 33.6 million people, at grave risk. They would have the least food stockpiled at home and be the first to need food supplies. A work force preoccupied with finding food would be unable to perform its normal jobs. Social order likely would decay if a food shortage were protracted. A government that cannot supply the population with enough food to preserve health and life could face anarchy.

In the event of a crisis, often merely in the event of bad weather, supermarket shelves are quickly stripped as some people begin to hoard food. Hoarding deprives government of the opportunity to ration local food supplies to ensure that all people are adequately fed in the event of a food shortage. The ability to promptly replenish supermarket food supplies becomes imperative in order to avoid mass hunger.

Blackouts of the electric grid caused by storms or accidents have destroyed food supplies. An EMP attack that damages the power grid and denies electricity to warehouses or that directly damages refrigeration and temperature control systems could destroy most of

the 30-day regional perishable food supply. Blackouts also have disrupted transportation systems and impeded the replenishment of local food supplies.

Federal, state, and local government agencies combined sometimes have had difficulty compensating for food shortages caused by storm-induced blackouts. For example:

- ◆ Hurricane Katrina in August 2005 caused a protracted blackout in New Orleans and the coastal region, destroying the food supply. Flooding, downed trees, and washed-out bridges paralyzed transportation. But the Katrina blackout by itself was sufficient to stop transportation and prevent rapid replenishment and repair of the food infrastructure because gas stations could not operate without electric power. An EMP attack could also paralyze transportation of food by rendering gas pumps inoperable, causing vehicles to fail and blacking out traffic lights, resulting in massive traffic jams. Hurricane Katrina's destruction of the food supply was a major contributing factor to the necessity of mass evacuation of New Orleans and the coastal population. Because many evacuees never returned, the protracted disruption of the food infrastructure, which lasted weeks—and in some localities months—while the electric power grid was being restored, was a major factor contributing to permanently reducing the populations of New Orleans and coastal Louisiana. Hurricane Katrina's effect on the food infrastructure is comparable to what can be expected from a small EMP attack.
- ◆ Hurricane Lili in October 2002 blacked out the power grid in coastal Louisiana, virtually collapsing the local food infrastructure. As a consequence of the blackout, food was unavailable to thousands through normal means. In south Louisiana, 30 supermarkets would not open because the blackout prevented their electric cash registers from operating. Those stores that did open were stripped of food within hours. In Abbeville, the parking lots of shopping centers became feeding stations run by churches and the state Office of Emergency Preparedness. Associated Grocers, which supplies food to supermarkets in Louisiana, Texas, and Mississippi, sent food in refrigerated trucks to the area from regional warehouses.

The food emergency was reflected in a skyrocketing demand for dry ice to preserve food stuffs during the hot weather and to preserve refrigerated foods. Local supplies of dry ice were exhausted quickly—one store selling 20,000 pounds of dry ice to hundreds of customers in 2 hours—and had to be supplemented with supplies from the Red Cross.

It is important to note that no one died from food or water deprivation during this emergency, and that the damaged area was small enough to be aided rapidly during recovery by undamaged fringe areas.

- ◆ Hurricane Floyd in September 1999 put more than 200 supermarkets out of operation in North Carolina. Protracted blackouts caused massive food spoilage despite emergency efforts taken before the storm to preserve perishable goods in freezers. Floyd blackouts also impeded replenishment of some supermarkets by inducing traffic signal failures that contributed to massive traffic jams.
- ◆ An ice storm blacked out the Washington, D.C., area in January 1999. Warm food, potentially a survival issue in the freezing winter conditions, was not available in most people's homes because electric ovens and microwaves no longer worked.

In addition, most gas-powered ovens would not work because those built since the mid-1980s have electronic ignition and cannot be lit with a match. Some resorted to cooking on camp stoves. Preserving refrigerated foods was also a concern that Pepco,

the regional power authority, helped address by giving away 120,000 pounds of dry ice, all that it had. Dry ice became a precious commodity.

- ◆ In January 1998, an ice storm caused a widespread blackout affecting parts of Ontario and Quebec in Canada, and Maine and upstate New York in the United States. The blackout threatened the food supply. According to press reports, “Food poisoning has become a real threat as embattled Montrealers, unable to get to stores, eat food that has been kept too long in refrigerators that no longer work.”

In upstate New York, the electric utility Niagara Mohawk announced that it was focusing restoration of electric power on more populated areas “so that supermarkets, gasoline stations, and hotels could reopen, and people in the more rural areas could find food and shelter.” New York State Electric and Gas helped customers get to shelters and distributed 200,000 pounds of dry ice for preserving food.

- ◆ Hurricane Andrew in August 1992 laid waste to 165 square miles in South Florida and left 3.3 million homes and businesses without electricity. Andrew’s aftermath posed an immediate threat to life in South Florida, in part because of damage to the food infrastructure. Most grocery stores had been destroyed.

Massive traffic jams, caused in part by nonfunctioning signal and street lights, prevented the surviving supermarkets from being resupplied. “More than 5,000 traffic lights are on the blink,” the press reported. “Traffic was snarled for miles. The simplest chore, indeed almost everything, seemed to take forever.”

To meet the crisis, tons of surplus food were distributed in the area. Nonetheless, two weeks after the hurricane, food was still not reaching many victims.

Andrew’s blackout of the power grid made the crisis over food, water, and shelter worse by severing communications between relief workers and victims. Without power, there was an almost complete collapse of communications—no telephones, radio, or television. Consequently, many people were unaware of relief efforts or of where to go for help. Had Hurricane Andrew damaged a larger area, it is likely that undamaged fringe areas would have been less capable of coming to the rescue, resulting in a significant loss of life.

Storm-induced blackouts provide some basis for extrapolating the greater destructive effects on food infrastructure likely from an EMP attack. An EMP attack is likely to damage electric power grids and other systems over a much wider geographic area than blackouts caused by storms; therefore, recovery from an EMP attack probably would take longer. An EMP attack also could directly damage some electronic systems, including refrigeration systems and vehicles, which normally would not be damaged by a blackout. Compared to blackouts, an EMP attack could inflict damage over a wider geographic area and damage a much wider array of equipment; consequently, recovery of the food infrastructure from EMP is likely to be much more complicated and more protracted.

Federal, state, and local agencies combined would find it difficult to cope immediately or even over a protracted period of days or weeks following an EMP attack that causes the food infrastructure to fail across a broad geographic area encompassing one or more states. Infrastructure failure at the level of food distribution because of disruption of the transportation system, as is likely during an EMP attack, could bring on food shortages affecting the general population in as little as 24 hours.



Massive traffic jams are most likely in large cities, the very areas where rapid replenishment of the food supply at hundreds of supermarkets will be needed most urgently. Significantly, recent famines in the developing world have occurred, despite massive relief efforts by the international community, in large part because food relief could not reach victim populations through their underdeveloped transportation infrastructure. An EMP attack could, in effect, temporarily create in the United States the technological conditions in the food and transportation infrastructures that have resulted in developing world famines.

## Recommendations

Current planning, as reflected in the President's National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, the Public Health, Security, and Bioterrorism Preparedness and Response Act of 2002 (the Bioterrorism Act), and Federal Emergency Management Agency (FEMA) planning documents, all appear to assume relatively small-scale threats to the food infrastructure. Most concern is focused on terrorists' poisoning or infecting a small portion of the food supply to cause mass panic and public fear about the safety of all food. The FEMA Federal Response Plan for a food shortage assumes a disaster effecting about 10,000 people: "On the fringes of the geographic areas affected will be schools and small institutions having large inventories estimated to be sufficient to feed up to 10,000 people for 3 days and supply their fluid needs for 1 day."<sup>1</sup> Yet an EMP attack could so damage the food infrastructure that millions of people would be at risk. Recommendations to address this risk include the following:

- ◆ Relevant federal agencies, including the Department of Homeland Security and the USDA, should supplement their plans to meet food emergencies by drawing on federal food stockpiles.
- ◆ Federal food stockpiles should be sized to meet a possible large-scale food shortage in the event of massive disruption of the national food infrastructure from an EMP attack or other causes.
- ◆ The Federal Government should examine useful lessons learned from reviewing earlier plans and programs, such as those during the early Cold War years, when the Federal Government planned and prepared for food shortages on a large scale.
- ◆ The Federal Government should plan to locate, preserve, deliver, distribute, and ration existing stockpiles of processed and unprocessed food, including food stockpiles by the USDA and other government agencies, which will be an important component of maintaining the food supply.
- ◆ The Federal Government should make it a priority to plan to protect, deliver, and ration food from regional warehouses, under conditions in which an EMP attack has disrupted the power, transportation, and other infrastructures for a protracted period.
- ◆ The Federal Government should make plans to process and deliver private and government grain stockpiles to significantly supplement the processed food stored in regional warehouses. According to the USDA's National Agricultural Statistical Service, total private grain stockpiles in the United States amount to more than 255 million metric tons. Federal grain stockpiles held by the Commodity Credit Corporation exceed 1.7

---

<sup>1</sup> FEMA, Response and Recovery, Emergency Support Function No. 11 Food Annex, <http://www.au.af.mil/au/awc/awcgate/frp/frpesf11.htm>.



million metric tons, with 1.6 million metric tons of that amount dedicated to the Bill Emerson Humanitarian Trust for overseas emergency.

- ◆ The Federal Government should increase food stockpiles if existing stockpiles of food appear to be inadequate.
- ◆ Contingency plans also should be made to provide significant levels of personnel and technical support to speed the recovery of agriculture and food production from an EMP attack.

Presidential initiatives have designated the Department of Homeland Security as the lead agency responsible for the security of the food infrastructure, overseeing and working with the USDA. Currently, under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (the *Stafford Act*) the President “is authorized and directed to assure that adequate stocks of food will be ready and conveniently available for emergency mass feeding or distribution” in the United States.<sup>2</sup> However, in practice, the *Stafford Act* has been used to authorize purchasing food from private sources and issuing food coupons to be used in supermarkets in order to meet food shortages.

In some particularly dire emergencies, as during Hurricane Katrina and Hurricane Andrew, when private sector food resources were destroyed or inadequate to meet the crisis, the Federal Government has resorted to federal surplus foods. Many Andrew victims were saved from hunger by Meals Ready to Eat (MRE). But the Federal Government was surprised by Andrew, and the resort to MREs and surplus food stockpiles was a poorly planned act of desperation that came late in the crisis. Recommendations to achieve this initiative include the following:

- ◆ The Federal Government should consider one readily available option, which is to grow the food stockpile to include the MREs.
- ◆ Plans should include timely distribution of mass quantities of food, which is likely to be crucial during a shortage.
- ◆ The *Stafford Act* should be amended to provide for plans to locate, protect, and distribute existing private and government stockpiles of food and to provide plans for distributing existing food stockpiles to the general population in the event of a national emergency.

---

<sup>2</sup> Appendix B, Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288, as amended (as of September 1, 1999), p. B-43, <http://www.fema.gov/pdf/government/grant/pa/pagappb.pdf>.

## Chapter 8. Water Infrastructure

### Introduction

Water and its system of supply is a vital infrastructure. High-altitude electromagnetic pulse (EMP) can damage or disrupt the infrastructure that supplies water to the population, agriculture, and industry of the United States (U.S.).

The water infrastructure depends for its operation on electricity. To the extent possible, aqueducts, tunnels, pipelines, and other water delivery systems are designed to rely on gravity. However, since the invention and proliferation of the electric water pump early in the last century, urban growth, planning, and architecture have been liberated from dependence on gravity-fed water systems. By making water move uphill, the gravity pump has made possible the construction and growth of cities and towns in locations that, in previous centuries, would have been impossible. Skyscrapers and high-rise buildings, which would be impractical if dependent on a gravity-fed water system, have been made possible by the electric pump.

Electrically driven pumps, valves, filters, and a wide variety of other electrical machinery are indispensable for the purification of water for drinking and industrial purposes and for delivering water to consumers. An EMP attack could degrade or damage these systems, affecting the delivery of water to a very large geographic region.

Electrical machinery is also indispensable to the removal and treatment of wastewater. An EMP attack that degraded the processes for removing and treating wastewater could quickly cause public health problems over a wide area.

Supervisory and Control Data Acquisition Systems (SCADA) are critical to the running and management of the infrastructure for delivery of pure water for drinking, for industry, and for the removal and treatment of wastewater. SCADAs enable centralized control and diagnostics of system problems and failures and have made possible the regulation and repair of the water infrastructure with a small fraction of the work force required in earlier days. As discussed in greater detail in Chapter 1, an EMP attack could damage or destroy SCADAs, making it difficult to manage the water infrastructure and to identify and diagnose system problems and overwhelming the small work force with systemwide electrical failures.

The electric power grid provides the energy that runs the water infrastructure. An EMP attack that disrupts or collapses the power grid would disrupt or stop the operation of the SCADAs and electrical machinery in the water infrastructure. Some water systems have emergency power generators, which could provide continued — albeit greatly reduced — water supply and wastewater operations for a short time.

Little analysis has been conducted of the potential vulnerability of the water infrastructure to EMP attack. However, SCADAs supporting the water infrastructure are known not to have been hardened, or in most cases even tested, against the effects of an EMP attack.

The electric power grid, on which the water infrastructure is critically dependent, is known to be vulnerable to feasible levels of EMP. Moreover, blackouts of the power grid induced by storms and mechanical failures are known to have disrupted the water infrastructure on numerous occasions. These storm- and accident-induced blackouts of the power grid are not likely to be as severe or as geographically widespread in their consequences for the water infrastructure as would an EMP attack.

Federal, state, and local emergency services, faced with the failure of the water infrastructure in a single large city, would be hard pressed to provide the population with the minimum water requirements necessary to sustain life over a time frame longer than a few days. They could not provide, on an extended emergency basis, the water requirements and services, including waste removal, necessary to sustain normal habitation and industrial production in a single large city; however, an EMP attack could disrupt the water infrastructure over a large geographic area encompassing many cities for a protracted period of weeks or even months.

### **The Water Works**

Water for consumption and sanitation is taken for granted by virtually everyone in the United States. Yet, the infrastructure for supplying pure water to the U.S. population and industry and for removing and treating wastewater, compared to other infrastructures, took longer to build and arguably is the most important of all infrastructures for the sustenance of human life.

One of the most important differences between developed and underdeveloped nations is the availability of pure water. An estimated 1.3 billion people in the developing world, nearly one-quarter of the global population, lack access to safe drinking water and even more, approximately 1.8 billion, lack water for sanitation. Consequently, diseases related to impure water flourish in many underdeveloped nations, taking a devastating toll on health and longevity. Economic development in many developing world nations is impeded by the absence of an adequate water supply to support industry. Indeed, in some countries, a major obstacle to development is simply the fact that the labor force has no alternative but to spend much of its time transporting water for drinking and other domestic uses from distant and often contaminated sources.

In contrast to the water scarcity that impedes development in much of the developing world, the United States enjoys a healthy and growing population and economic prosperity supported by the efficient distribution and utilization of its abundant water resources. Freshwater consumption for all purposes averages about 1,300 gallons per capita per day in the United States. Irrigation and cooling account for about 80 percent of all consumption, and, in the 17 western states, irrigation alone accounts for more than 80 percent of water consumption. On average, some 100 gallons per person per day (200 gallons per person per day in the southwest) are consumed for domestic purposes such as drinking, bathing, preparing food, washing clothes and dishes, flushing toilets, washing cars, and watering lawns and gardens.

Drinking and cooking account for only a small fraction of the water consumed; however, because in most cases a single water source must serve all purposes, all water consumed, regardless of the purpose, must meet the standards for drinking water purity, as prescribed by law.

Supporting this demand for enormous quantities of high-quality water is a vast infrastructure that includes more than 75,000 dams and reservoirs; thousands of miles of pipes, aqueducts, and water distribution and sewer lines; 168,000 drinking water treatment facilities; and 19,500 wastewater treatment facilities.

A fairly small number of large drinking water and wastewater utilities located primarily in urban areas (about 15 percent of the systems) provide water services to more than 75 percent of the U.S. population.

There is no single organization or system controlling the entire water infrastructure of the United States. Rather, more than 100,000 utilities and private owners manage the national water infrastructure. However, because water utilities provide similar services and must meet similar standards, they all operate in much the same way.

Water supplies require collection, treatment, storage, and distribution. Surface water such as reservoirs, lakes, and rivers generally provides water for cities. Wells tapping underground aquifers often supply rural areas and the southwestern states. Homeowners with private wells typically drink the water directly, because the subsurface water has been filtered over many years within the natural underground sedimentation. Water treatment plants are designed to provide an uninterrupted water supply that raises the purity of surface water and aquifers to drinking standards. A typical municipal water treatment plant purifies water through several steps: filtration, coagulation, flocculation, sedimentation, and disinfection.

Filtration by utilities passes raw water first through coarse filters to remove sticks, leaves, and other large debris. Finer filtration passes water through layers of sand and other granular material to remove silt and microorganisms. This stage of treatment imitates the natural filtration of water as it moves through the ground. This entire process is accomplished through low-lift pumps and mechanically cleaned bar screens and fine screens.

Coagulation is the process of removing colloidal impurities, finely suspended particles, from the filtered water. A coagulant, such as aluminum sulfate, is thoroughly mixed into water containing colloidal particles. Aluminum sulfate not only will coagulate and remove colloidal particles, but also will react with calcium hydroxide in the water, forming aluminum hydroxide, which can be removed through further filtration or sedimentation.

Flocculation immediately follows the coagulation process to remove the finest particles that would never settle out naturally. The velocity of the water is reduced and a gentle mixing action is used to allow formation of insoluble salts, colloidal particles, and other remaining suspended matter into a “floc” particle. The colloids and the coagulants mix with each other to form a large neutral floc particle that will settle out during sedimentation.

Sedimentation involves moving the water to large tanks to allow the floc to settle to the bottom of the tank. Sedimentation basins or clarifiers are usually the largest tanks in the treatment process. About 1 pound of sludge is created for every pound of chemical added to the water for coagulation and flocculation. The sludge must be removed and disposed of and filters and screens must be backwashed regularly.

Disinfection uses chemicals to kill any microorganisms that may have survived the filtration process. Chlorine is the most common disinfectant. When chlorine combines with organic material, such as dead leaves, it produces potentially dangerous trihalomethanes (THM). Large water treatment plants in major cities often undertake an additional purification step that reduces the level of THMs. Ozone oxidation and ultraviolet light are other disinfectant processes that are sometimes used instead of or in addition to chlorine. Fluoride also may be added because of its ability to retard tooth decay. Groundwater is often aerated by bubbling air through the water or by spraying to oxidize dissolved iron and manganese and to remove odors caused by hydrogen sulfide.

Treated water is delivered by high-lift pumps to the distribution system, usually through pipelines pressurized to 40 to 80 psi, to consumers. These pumps help to maintain water levels in storage reservoirs. Gravity flow, whenever possible, is the preferred method for delivering water. However, most water must be delivered by means of electric pumps. High-pressure pumps at the treatment plant deliver water to various zones within a water district to a booster pump or series of booster pumps that completes delivery to the consumer. High-rise buildings typically are serviced by individual booster pumps with enough pressure to provide water to rooftop reservoirs for consumption by upper floors and to provide water for firefighting.

Many of the same processes used in purification of drinking water also are used in treatment of wastewater, suitably modified for the removal of the greater amounts of material found in sewage. Sewage provides an ideal environment for a vast array of microbes, primarily bacteria, plus some viruses and protozoa. In fact, wastewater processing relies on benign microorganisms in the purification process. Sewage may also contain pathogens from the excreta of people with infectious diseases that can be transmitted by contaminated water. Waterborne diseases, while seldom a problem now in developed nations, are still a threat in developing countries where treated water is not available for public use.

Contaminants are generally removed from wastewater physically, biologically, and chemically. First, rags, sticks, and large solids are removed by coarse screens to protect the pumps. Then grit, the material that wears out equipment, is settled out in grit tanks or chambers. At this point, most of the small solids are still in suspension and can be removed and concentrated in the primary gravity settling tanks. The concentrated solids, called raw sludge, are pumped to an anaerobic digester for biological decomposition. The clarified effluent then flows to secondary treatment units for biological oxidation where the dissolved and colloidal matter in wastewater provides nutrients for microorganisms. A final gravity settling tank is used to remove microorganisms. This concentrated biological sludge is removed and returned to the anaerobic digester. Chemical disinfection, usually employing chlorine, is the last stage in the treatment of wastewater before it is discharged.

### **Vulnerability to EMP**

The water infrastructure is a vast machine, powered partly by gravity but mostly by electricity. Electrically driven pumps, valves, filters, and a wide variety of other machinery and control mechanisms purify and deliver water to consumers and remove wastewater. An EMP attack could damage or destroy these systems, cutting off the water supply or poisoning the water supply with chemicals and pathogens from wastewater. For example:

- ◆ Total organic carbon (TOC) analyzers detect the levels of pollutants and pathogens in water. Determining water quality and the kind of purification treatment necessary depends on these sensors.
- ◆ Mechanical screens, filters, collector chains, skimmers, and backwash systems remove sludge and other solid wastes. Failure of these systems would pollute the water and quickly clog the pumps.
- ◆ SCADA systems enable remote control and instantaneous correction of potential problems with water quality, delivery, and wastewater removal and treatment. This process allows most water utilities to be nearly autonomous in operation, using a minimum



number of personnel. In an emergency, such as an electrical blackout, some subsystems have been or could easily be modified for workarounds. For example, many valves have a manual bypass mode, and some water plants have emergency power generators. However, the efficiencies made possible by SCADAs have reduced the available number of trained personnel probably below the levels required for protracted manual operation of water treatment facilities. The failure of SCADAs would greatly impede all operations.

- ◆ High-lift and low-lift pumps are ubiquitous throughout the infrastructure for purifying and delivering water and removing wastewater. Water cannot be purified or delivered, nor sewage removed and treated, if these systems are damaged or destroyed.
- ◆ Paddle flocculators and other types of mixers are the primary means of chlorination and other chemical purification. If these systems cease functioning, water cannot be purified and likely would remain hazardous.

All of these systems depend on the electric grid for power. Large water treatment plants consume so much electricity, in some cases about 100 megawatts, that backup generators are impractical. For reliability, water treatment plants typically draw electricity from two local power plants. An EMP attack that collapses the electric power grid will also collapse the water infrastructure.

### **Consequences of Water Infrastructure Failure**

By disrupting the water infrastructure, an EMP attack could pose a major threat to life, industrial activity, and social order. Denial of water can cause death in 3 to 4 days, depending on the climate and level of activity.

Stores typically stock enough consumable liquids to supply the normal demands of the local population for 1 to 3 days, although the demand for water and other consumable liquids would greatly increase if tap water were no longer available. Local water supplies would quickly disappear. Resupplying local stores with water would be difficult in the aftermath of an EMP attack that disrupts transportation systems, a likely condition if all critical infrastructures were disrupted.

People are likely to resort to drinking from lakes, streams, ponds, and other sources of surface water. Most surface water, especially in urban areas, is contaminated with wastes and pathogens and could cause serious illness if consumed. If water treatment and sewage plants cease operating, the concentration of wastes in surface water will certainly increase dramatically and make the risks of consuming surface water more hazardous.

One possible consequence of the failure of water treatment and sewage plants could be the release of sludge and other concentrated wastes and pathogens. Typical industrial wastes include cyanide, arsenic, mercury, cadmium, and other toxic chemicals.

Boiling water for purification would be difficult in the absence of electricity. Even most modern gas stoves require electricity for ignition and cannot be lighted by match. In any event, gas also may not be available to light the stoves (see Chapter 5). Boiling could be accomplished by open fires, fueled by wood or other flammables. Other possible mitigators are hand-held pump filters, water purification kits, iodine tablets, or a few drops of household bleach.

A prolonged water shortage may quickly lead to serious consequences. People preoccupied with finding or producing enough drinking water to sustain life would be unavailable to work at normal jobs. Most industrial processes require large quantities of water and would cease if the water infrastructure were to fail.

---



Demoralization and deterioration of social order can be expected to deepen if a water shortage is protracted. Anarchy will certainly loom if government cannot supply the population with enough water to preserve health and life.

The many homeowners with private wells also would face similar problems. There would be fewer workarounds to get their pumps operating again, if the pump controller is damaged or inoperable. Even if power is restored, it is unlikely the average homeowner would be technically competent to bypass a failed pump controller and figure out how to power the pump with bypass power lines.

The first priority would be meeting personal water needs. Federal, state, and local governments do not have the collective capability, if the water infrastructure fails over a large area, to supply enough water to the civilian population to preserve life.

Storm-induced blackouts of the electric grid have demonstrated that, in the absence of electric power, the water infrastructure will fail. Storm-induced blackouts have also demonstrated that, even in the face of merely local and small-scale failure of the water infrastructure, the combined efforts of government agencies at all levels are hard pressed to help. For example:

- ◆ Hurricane Katrina in August 2005 collapsed the water infrastructure in New Orleans and coastal Louisiana. The Katrina-induced blackout stopped the vast machinery for purifying and delivering water to the population. Water supplies were contaminated. The National Guard, among other resources, had to be mobilized to rush water and mobile water purification systems to the afflicted region. The water crisis—which was protracted because the blackout was protracted, the electric power grid requiring weeks and in some places months to repair—was a major contributing factor to the mass evacuation of the regional population. Once evacuated, many never returned. Thus the loss of water resources was a significant factor contributing to permanently reducing the population in the region. The effects of Hurricane Katrina on the water infrastructure are comparable to what can be expected from a small EMP attack.
- ◆ Hurricane Lili in October 2002 blacked out the power grid in coastal Louisiana. With no electricity, water pumps no longer worked, depriving the population of running water. Local bottled water supplies were quickly exhausted. Federal and state authorities resorted to using roadside parking lots and tanker trucks as water distribution centers.
- ◆ In September 1999, Hurricane Floyd blacked out electricity, causing water treatment and sewage plants to fail in some Virginia localities and, most notably, in Baltimore, Maryland. For several days, blackout-induced failure of Baltimore's Hampden sewage facility raised concerns about public health. With its three pumps inoperable, Hampden spilled 24 million gallons of waste into Baltimore's Jones Falls waterway and the Inner Harbor.
- ◆ An ice storm in January 1999 blacked out Canada's Ontario and Quebec provinces, causing an immediate and life-threatening emergency in Montreal's water supply, which depends on electricity for filtration and pumping. On January 9, the two water treatment plants that served 1.5 million people in the Montreal region failed, leaving the area with only enough water to last 4 to 8 hours. Government officials kept the water crisis secret, fearing public knowledge would exacerbate the crisis by water hoarding and panic. But as household water pipes went dry and reports of a water shortage spread, hoarding happened anyway and bottled water disappeared from

stores. Warnings not to drink water without boiling it proved pointless, because people had no other way of getting water and no way to boil it in the mid-winter blackout.

Montreal officials feared not only a shortage of drinking water, but also an inadequate supply of water for fighting fires. The Montreal fire department prepared to fight fires with a demolition crane instead of water, hoping that, if a building caught fire, the conflagration might be contained by demolishing surrounding structures. So desperate was the situation that provincial officials considered evacuating the city. Fortunately, Hydro-Quebec, the government's electric utility, managed to restore power to the filtration plants and restore water service before such extreme measures became necessary.

- ◆ In August 1996, a heat wave blacked out parts of the southwestern United States. Water supplies were interrupted in some regions because electric pumps would not work. Arizona, New Mexico, Oregon, Nevada, Texas, and Idaho experienced blackout-induced disruption in water service during the heat wave. In Fresno, where most of the city received water from wells powered by electric pumps, the city manager declared a local emergency. Only two of the city's 16 fire stations had water, and most of the fire hydrants were dry. Tankers were rushed in to supplement the fire department's water supply.
- ◆ Hurricane Andrew in August 1992 caused a blackout in South Florida that stopped water pumps from working. The blackout denied running water to hundreds of thousands of people stranded among the ruins left by Andrew, amidst Florida's summer heat. To meet the immediate crisis more than 200,000 gallons of water were distributed. However, without electricity to power radio or television sets, mass communication virtually ceased to exist, and people were unaware of relief efforts or where to seek help. Thousands may have been saved from dehydration by pyramids of bottled water on street corners made free for the taking and by survivors who spread the word.

In all the examples cited, timely emergency services to provide water prevented loss of life from dehydration. However, had the outages lasted longer and the blacked-out areas been larger, the outcome could have been very different. Storms are merely suggestive of, and provide some basis for extrapolating, the greater destructive effects on water infrastructure likely from an EMP attack.

Storm-induced blackouts and their effects on the water infrastructure are an imperfect analogy to EMP attack. Taken at face value, storm-induced blackouts and their consequences for the water infrastructure grossly understate the threat posed by an EMP attack. Storms are much more limited in geographic scope compared to an EMP attack. Power grid and water infrastructure recovery from storms, compared to recovery from an EMP attack, is likely to happen more quickly because of the "edge effect"—the capability of neighboring localities and states to provide recovery assistance. Because an EMP attack is likely to damage or disrupt electronics over a much wider geographic area than storm-induced blackouts, rescuers from neighboring states and localities would face a much bigger job, and recovery of the water infrastructure would take a much longer time.

Nor do storm-induced blackouts replicate the damage from an EMP attack that may occur in small-scale electronic systems critical to the operation of the water infrastructure, such as electric pumps, SCADAs, and motor controls for filters and valves. Compared to storms, an EMP attack is likely to inflict not only more widespread damage geo-

graphically, but also deeper damage, affecting a much broader array of electronic equipment, which will contribute to a more complicated and protracted period of recovery.

## Recommendations

A Presidential Directive establishes new national policy for protection of our nation's critical infrastructures against terrorist threats that could cause catastrophic health effects. National-level responsibilities have already been assigned to the Department of Homeland Security (DHS) and the Environmental Protection Agency (EPA) to protect the water infrastructure from terrorist threats. The EPA is the designated lead agency for protection of drinking water and water treatment systems. Under this directive:

- ◆ DHS and EPA should ensure that protection includes EMP attack among the recognized threats to the water infrastructure.
- ◆ The following initiatives should be amended:
  - The President's *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003), which details a plan for protecting the United States' critical infrastructures, including the infrastructure for water. The President's plan:
    - Identifies threats to the water infrastructure as: "Physical damage or destruction of critical assets...actual or threatened contamination of the water supply...cyber attack on information management systems...interruption of services from another infrastructure."
    - Directs the EPA to work with the DHS, state and local governments, and the water sector industry to: "Identify high-priority vulnerabilities and improve site security...improve sector monitoring and analytic capabilities...improve sector-wide information exchange and coordinate contingency planning...work with other sectors to manage unique risks resulting from interdependencies."
    - Focuses on terrorism and threats other than EMP, but lends itself well (in particular, its structure and logic) to addressing any threat, and should be amended to include EMP.
  - The *Public Health and Bioterrorism Preparedness and Response Act of 2002* (*Bioterrorism Act*), signed into law by President Bush on June 12, 2002. The Bioterrorism Act:
    - Requires the authorities over many drinking water systems to conduct vulnerability assessments, certify and submit copies of their assessments to the EPA, and prepare or revise their emergency response plans.
    - Is concerned with terrorist contamination of drinking water with chemical or biological agents.
    - Could be amended to address the greater bio-chemical threat that an EMP attack potentially poses to the water supply than any of the threats envisioned in the *Bioterrorism Act* because an EMP attack that causes SCADAs in water treatment facilities to malfunction could release biochemical agents, and conceivably contaminate water supplies over a very wide region.
- ◆ DHS and EPA should follow the government-recommended emergency preparedness steps applicable to a wide range of civil emergencies arising from different threats. These steps include assuring availability of water during emergencies. To that end, the government has recommended that citizens stockpile both water supplies and means of purification. Implementing these recommendations will provide some measure of preparation for an EMP threat to the water supply.

## Chapter 9. Emergency Services

### Introduction

Emergency services are essential to the preservation of law and order, maintenance of public health and safety, and protection of property. Americans have come to rely on prompt and effective delivery of fire, police, rescue, and emergency medical services through local government systems. Backing up these local systems are state capabilities (e.g., state police and National Guard) and specialized capabilities such as those provided by the Department of Homeland Security (DHS), the Department of Justice, the Centers for Disease Control and Prevention, and other federal entities.

*Americans have come to rely on prompt and effective delivery of fire, police, rescue, and emergency medical services.*

The demand for emergency services is large. Across the United States more than 200 million 9-1-1 calls are fielded annually.<sup>1</sup> Responding to these calls is an army of some 600,000 local law enforcement officers, 1 million firefighters, and more than 170,000 emergency medical technicians and paramedics.<sup>2</sup> Anticipated expenditures over the next 5 years for emergency response services are estimated at \$26 billion to \$76 billion at the state and local levels, supplemented by an additional \$27 billion at the federal level.<sup>3</sup>

Emergency services at all levels are receiving increased emphasis as a consequence of the September 11, 2001, terrorist attacks. The focus is on preventing and responding to terrorism, including nuclear attack, but little emergency services planning specifically considers electromagnetic pulse (EMP) attack.

*Little emergency services planning specifically considers EMP attack.*

The primary focus in this chapter is on local emergency services systems. In particular, this chapter focuses on the communications systems to alert, dispatch, and monitor those emergency services. The great majority of resources are concentrated at the local level; state and federal assistance will likely be quite thin, given the large geographic extent of an EMP attack.

In addition to local emergency systems, we also address the federal Emergency Alert System (EAS), designed to serve the President and other leaders in communicating with the public in emergency situations. Although no President has ever used the EAS, it is reasonable to anticipate that it would be used in the event of an EMP attack.

### Emergency Services Systems Architecture and Operations

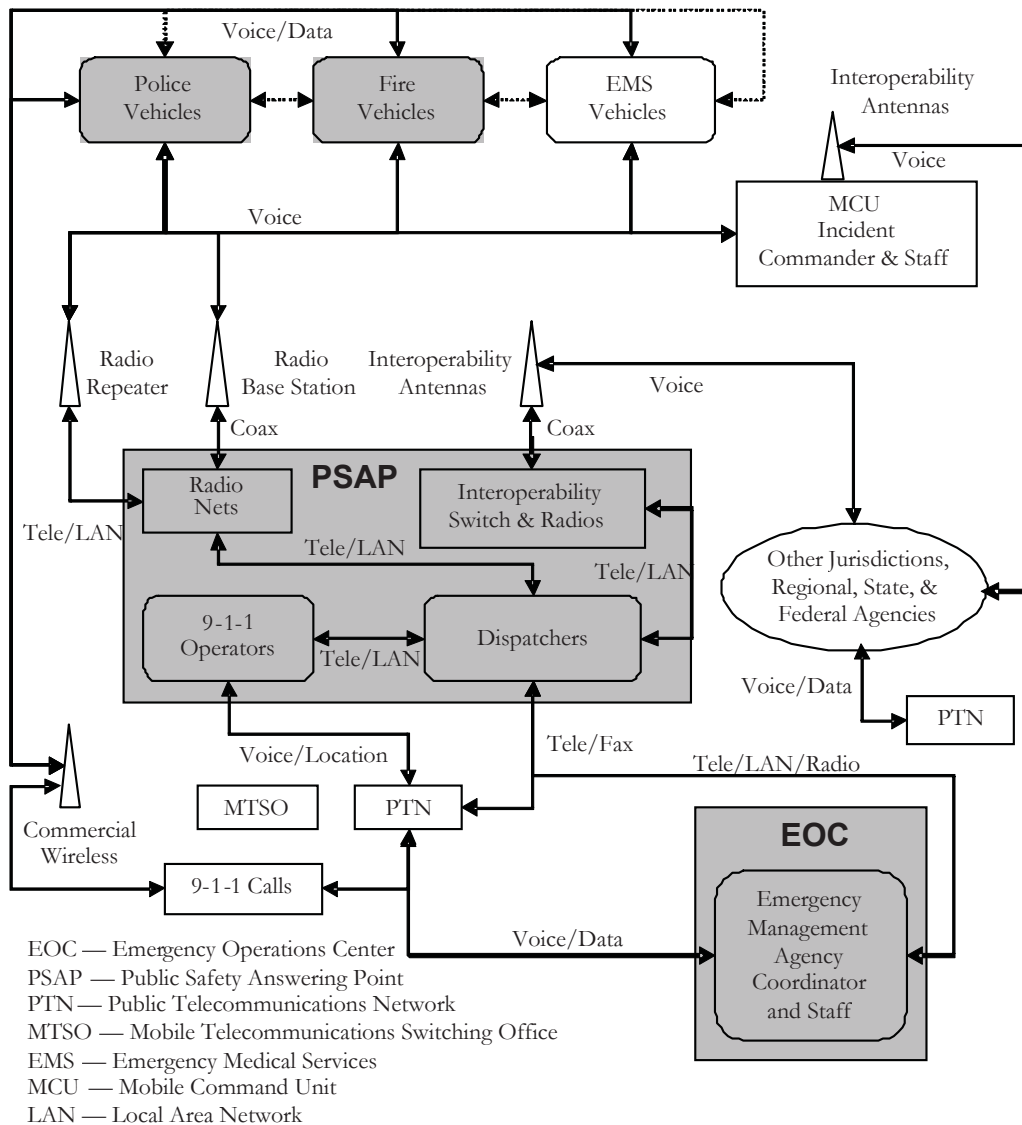
#### Local Emergency Services Systems

**Figure 9-1** depicts a generic modern local emergency service system. Shaded elements are those for which we have assessed EMP vulnerability, as discussed later in this chapter.

<sup>1</sup> National Emergency Number Association.

<sup>2</sup> Bureau of Labor Statistics. Frontline workers, including volunteers; excludes supervisory personnel.

<sup>3</sup> Rudman, Warren B., et al., *Emergency Responders: Drastically Underfunded, Dangerously Unprepared*, Council on Foreign Relations, 2003.



**Figure 9-1. A Generic Modern Emergency Services System**

Calls for assistance come in on cellular and land telephone lines to 9-1-1 operators at centers known as Public Safety Answering Points (PSAP). PSAPs typically include one or more 9-1-1 operators and dispatchers, communications equipment, computer terminals, and network servers. The 9-1-1 operator determines the service required and forwards the information for dispatch of the appropriate response units.

In addition to standard landline telephone service, emergency services employ a variety of wireless communication systems, including radio systems, cellular and satellite telephone systems, paging systems, messaging systems, and personal digital assistants. Because of dead zones and restrictions on radiated power levels in communications paths, radio repeaters are often used to relay voice and message traffic.

Because networks in nearby communities generally operate on different frequencies or channels to avoid interference, PSAP personnel use special equipment to handle community-to-community communications. If an emergency or public safety activity requires close and continuous coordination among several communities or agencies, an interoper-



erability switch is used to allow direct communications among organizations. Interoperable communications across separate political jurisdictions is still a problem and under development in most regions.

For more serious emergencies, the Emergency Operations Center (EOC) serves as a central communications and coordination facility to which multiple organizations can send representatives. It facilitates efficient coordination across emergency services departments and state and federal agencies.

### **The Emergency Alert System**

The original motivation for the EAS (previously the Emergency Broadcast System and initially Control of Electromagnetic Radiation [CONELRAD]) was to provide the President the ability to communicate directly with the American people in time of crisis, especially enemy attack. Although it has never been used for that purpose, it has been activated in local emergencies and is widely used for weather alerts. The Federal Communications Commission (FCC) sets requirements through regulation of television and radio stations. The Federal Emergency Management Agency (FEMA), now part of DHS, provides administrative oversight.

In the case of a national emergency, a message is relayed from the President or his agent to high-power amplitude modulation (AM) radio stations, known as national primary stations, across the country. These stations broadcast signals to other AM and frequency modulation (FM) radio stations, weather radio channels, and television stations that, in turn, relay the message to still other stations, including cable television stations. These stations use encoders and decoders to send and receive data recognized as emergency messages.

### **Impact of an EMP Attack**

In a crisis, the priorities for emergency services are protection of lives, protection of property, effective communication with the public, maintenance of an operational EOC, effective communication among emergency workers, and rapid restoration of lost infrastructure capabilities. An EMP attack will adversely affect emergency services' ability to accomplish these objectives in two distinct ways: by increasing the demand for services and by decreasing the ability to deliver them.

### **Demand for Emergency Services**

The demand for emergency services will almost certainly increase dramatically in the aftermath of an EMP attack. These demands fall into two broad categories: *information* and *assistance*. The absence of timely information and the inability of recovery actions to meet the demand for emergency services will have grave consequences.

◆  
*The demand for emergency services will almost certainly increase dramatically in the aftermath of an EMP attack.*

Large-scale natural and technological disasters that have occurred in the last several decades demonstrate that information demands are among the first priorities of disaster victims. At the onset of a disaster, an individual is concerned primarily with his or her personal well-being and that of close family members and friends. The next most pressing concern is for information regarding the event itself. What happened? How extensive is the damage? Who was responsible? Is the attack over? A less immediate priority is for



information regarding recovery. How long will it take to restore essential services? What can and should I do for self-preservation and to contribute to recovery? It is important to recognize that emergency services providers also need all this information, for the same reasons as everyone else and also to manage recovery operations efficiently and perform their missions. Information assurance for emergency services requires reliable communications supporting the transport of emergency services such as enhanced 9-1-1 (E9-1-1).<sup>4</sup> As discussed in Chapter 3, Telecommunications:

Based upon results of the Commission-sponsored analysis, an EMP attack would disrupt or damage a functionally significant fraction of the electronic circuits in the Nation's civilian telecommunications systems in the region exposed to EMP. The remaining operational networks would be subjected to high levels of call attempts for some period of time after the attack, leading to degraded telecommunications services.

To meet the demand for priority national security and emergency preparedness (NS/EP) services supporting first responders, the FCC and the DHS's National Communications System (NCS) offer a wide range of NS/EP communications services that support qualifying federal, state, and local government, industry, and nonprofit organization personnel in performing their NS/EP missions, including E9-1-1 PSAPs.<sup>5,6</sup>

The demand for assistance will increase greatly in the event of an EMP attack. The possibility of fires caused by electrical arcing resulting from an EMP attack cannot be ruled out. There is no reliable methodology to predict the frequency of such fires. As with other EMP effects, however, they will occur near-simultaneously, so that even a small number could overwhelm local fire departments' ability to respond. Fires indirectly caused by an EMP attack, principally because of people being careless with candles used for emergency lighting or with alternative heating sources during power blackouts, are also a concern.

There also exists the possibility of EMP-caused airplane crashes.<sup>7</sup> The average daily peak of air traffic in U.S. airspace includes more than 6,000 commercial aircraft carrying some 300,000 passengers and crew. Commercial aircraft are protected against lightning strikes but not specifically against EMP. The frequency composition of lightning and EMP differ enough so that lightning protection does not ensure EMP protection. On the other hand, the margins of safety for lightning protection imposed on commercial aircraft may provide flight safety in the event of an EMP attack. In any event, we cannot rule out the possibility of airplane crashes.

Debilitating EMP effects on the air traffic control system will also be a contributing factor to airplane crashes.

Emergency rescue services can be expected to experience an increase in demand. People trapped on subways and in elevators will require timely rescue. If electric power is interrupted for any period of time, people at home who depend on oxygen concentrators, respirators, aspirators, and other life-sustaining equipment that require electric power will need to find alternative solutions quickly. Home backup systems, including oxygen tanks, liquid oxygen supplies, and battery and generator power, will lessen the need for an

<sup>4</sup> E9-1-1 provides emergency services personnel with geographic location information on mobile callers.

<sup>5</sup> PSAP Enrollment in the TSP Program, <http://www.nasna911.org/pdf/tsp-enroll-guide.pdf>.

<sup>6</sup> National Communication System, <http://www.ncs.gov/services.html>.

<sup>7</sup> See also Chapter 6, Transportation Infrastructure.

immediate response for those fortunate enough to have them, but eventually all these people will need to be transported to facilities with a reliable power source and appropriate equipment. If power is out for more than several days, people dependent on dialysis machines, nebulizers, and other life-supporting medical devices also will be at risk. Finally, inability to replenish home supplies of medicines will eventually lead still more people to depend on emergency services.

Police services will be stretched extremely thin because of a combination of factors. Police will be called on to assist rescue workers in removing people from immediate dangers. Failures of automobiles and traffic control systems with attendant massive traffic jams will generate demands for police services for traffic management. Antisocial behavior also can occur following a chaotic event. Though it is more commonly seen in disasters originating from conflict, such as riots, than from natural or technological disasters, opportunistic crime (because of failures of electronic security devices, for example) is a potential reaction to an EMP attack. While not as prevalent as may be perceived, far worse antisocial behavior such as looting also could occur, especially in communities that experience conflict because of shortages or in areas that experience high crime rates under nondisaster circumstances. If looting or other forms of civil disorder break out, it is likely that local police services will be overwhelmed. In that event, deployment of National Guard forces, imposition of curfews, and other more drastic measures may be necessary.

Although emergency services could be completely overwhelmed in the aftermath of an EMP attack, it is important to recognize that the demand for emergency services could be ameliorated somewhat

◆  
*Emergency services could be completely overwhelmed in the aftermath of an EMP attack.*

by citizen groups that frequently emerge in the aftermath of disasters to lead or assist in recovery efforts. In the absence or failure of government-provided emergency services, these groups may take on roles similar to those services, for example, by moving and providing basic household necessities to families in need, clearing debris, or serving as an impromptu communications network. This example of prosocial behavior is not uncommon in the aftermath of natural disasters such as hurricanes, floods, or earthquakes. This was seen following the September 11, 2001, terrorist attacks, when thousands of New York citizens volunteered to give blood, help firefighters and police at the World Trade Center grounds, and assist in other ways.

On the other hand, when the failure of police and emergency services becomes protracted, the lawless element of society may emerge. For example, Hurricane Katrina in August 2005 damaged cell phone towers and radio antennas that were crucial to the operation of emergency communications. Protracted blackout of the power grid caused generators supporting emergency communications to exhaust their fuel supplies or fail from overuse. Consequently, government, police, and emergency services were severely impacted in their ability to communicate with the public and with each other. Looting, violence, and other criminal activities were serious problems in the aftermath of Katrina. In one instance, the Danziger Bridge incident<sup>8</sup>, members of a repair crew came under fire. Police called to the scene returned fire, and a number of people were killed. An EMP

---

<sup>8</sup> Burnett, John. "What Happened on New Orleans's Danziger Bridge?" <http://www.npr.org/templates/story/story.php?storyId=6063982>.

attack is likely to incapacitate the same nodes—cell phone towers and radio antennas—and overtax generators supporting emergency communications for a protracted period, creating the same conditions that incited lawless behavior in the aftermath of Katrina.

### **EMP Effects on Emergency Services**

Some equipment needed to perform emergency services will be temporarily upset or directly damaged by an EMP attack, resulting in diminished capabilities during the time of greatest demand.

*An EMP attack will result in diminished capabilities during the time of greatest demand.*

Little, if any, emergency services equipment has been hardened specifically against EMP and thus may be vulnerable. On one hand, both communications equipment and vehicles commonly employed in the emergency services infrastructure generally have been designed to cope with the increasingly dense everyday electromagnetic environment from radio, television, wireless communications, radar, and other man-made sources. On the other hand, emergency services rely on radios to transmit and receive voice and message traffic using many frequencies, including the same frequencies contained in EMP radiation fields. Whether or not this results in degradation depends on the effectiveness of any built-in protection devices in these radios as well as the internal robustness of the radio itself.

To gauge the degree of vulnerability of emergency services to EMP, the Commission conducted an assessment of emergency services equipment and associated networks.<sup>9</sup> We tested a representative variety of key electronics-based equipment needed by national leadership, first responders, and the general population. In most cases, only one of each model was tested, so statistical inferences are not possible from our test data. Moreover, a more robust assessment would test equipment under a range of conditions (such as different orientations, equipment operating modes, and test waveforms). Thus, our assessment should be viewed as indicative, rather than definitive. Notwithstanding these caveats, these tests are the most comprehensive recent vulnerability tests of emergency services equipment to date.

Our testing concentrated on items that were found to be critical for local emergency services and the EAS. The testing used standard EMP test practices, including radiated pulse and direct current injection test methods. Large-scale and smaller radiated pulse simulators were used to illuminate the equipment with an approximation of the electromagnetic field generated by an actual EMP event. A second test method, known as pulse current injection, accounted for the stresses coupled to long lines such as power feeds that cannot be accurately tested in a radiated simulator. We also used the results of relevant past EMP testing efforts.

**Public Safety Answering Points.** The key elements of a PSAP include commercial telephone links for incoming 9-1-1 calls, computer-aided dispatch, public safety radio, and mobile data communications. There are other elements associated with PSAPs, but this is the minimal set necessary to provide emergency response to the public.

Computers are essential to normal PSAP operations. Recent personal computer equipment tests covered a wide technology range, consistent with what is typically in use in

<sup>9</sup> Radasky, William A., *The Threat of Intentional Electromagnetic Interference (IEMI) to Wired and Wireless Systems*. Metatech Corporation, Goleta, California, 162.

PSAPs. Results indicate that some computer failures can be expected at relatively low EMP field levels of 3 to 6 kilovolts per meter (kV/m). At higher field levels, additional failures are likely in computers, routers, network switches, and keyboards embedded in the computer-aided dispatch, public safety radio, and mobile data communications equipment.

A variety of mobile radios were tested in the stored, dormant, and operating states, in both handheld and vehicle-mounted configurations. Consistent with older test data,<sup>10</sup> none of the radios showed any damage with EMP fields up to 50 kV/m. While many of the operating radios experienced latching upsets at 50 kV/m field levels, these were correctable by turning power off and then on. However, most of the fixed installation public safety radio systems include telecommunication links between the computer-aided dispatch terminals and the main or repeater radio units. Therefore, because of computer failures in dispatch equipment, communication system failures might occur at EMP field levels as low as 3 to 6 kV/m.

Based on these results, we anticipate that several major functions of PSAPs will be affected by an EMP attack. The significance and duration of the impact of these failures will depend on multiple factors such as the ability of technical staff to repair or replace damaged equipment and the existence of plans and procedures to cope with the specific type of failure. For example, based on a review of representative Y2K public safety contingency plans, loss of the computer-aided dispatch capability can be overcome by the use of simple note cards for manually recording the information needed for dispatch. However, loss of the mobile radio communications or the incoming commercial telecommunications functions could be more difficult to counteract. Typically, local jurisdictions rely on nearby PSAPs or alternate locations to overcome these types of failures. In an EMP attack, these contingency plans may fail because of the wide area of effects.

***Interoperability Switches.*** These switches are contained in many PSAPs to facilitate direct communications among local, regional, and state public safety departments and federal agencies after major disasters. The main elements of the interoperability switch capability are the public safety radios, the switch unit itself, and the computer network link between the switch unit and the dispatch console. The public safety radios that were tested as part of this assessment were based on the equipment used in a fully operational interoperability switch.<sup>11</sup> The testing was performed with the equipment in stored, dormant, and operating states. No failures were experienced at test levels up to 50 kV/m. The interoperability switch was also tested up to 50 kV/m with no adverse effects.

Based on these results, the interoperability switch capability is expected to function normally after an EMP attack. However, the computer network link between the interoperability switch and the dispatch station may fail at field levels as low as 3 to 6 kV/m. This would necessitate manual operation of the switch to implement the connections among various law enforcement, fire, and EMS agencies.

***Vehicles.*** Emergency service vehicles include police cars, fire trucks, and EMS vehicles. An extensive test of a police car was performed. The most severe effect found

---

<sup>10</sup> Barnes, Paul R., *The Effects of Electromagnetic Pulse (EMP) on State and Local Radio Communications*, Oak Ridge National Laboratory, October 1973.

<sup>11</sup> Metropolitan Interoperability Radio System — Alexandria Site Description Document, *Advanced Generation of Interoperability for Law Enforcement (AGILE)*, Report No. TE-02-03, April 4, 2003.

was the latch-up of a mobile data computer at approximately 70 kV/m. After rebooting, the computer functioned normally.

Electronic equipment found on many of the mobile units also was tested. This equipment included a computer, personal data assistant, mobile and portable radios, defibrillators, and vital signs monitors. No permanent failures were experienced at levels up to 70 kV/m. Thus, we anticipate that the electronics in emergency services mobile units will continue to function normally, but they may suffer some initial effects due to latching upset of electronic devices.

*Emergency Operation Centers.* A site survey was performed at the Virginia state EOC. The survey confirmed that the vast majority of EOC communications depends on the Public Telecommunications Network (PTN). Thus, the ability of the EOC personnel to communicate and therefore provide emergency coordination will be highly dependent on the capability of the public telecommunications infrastructure to operate after an EMP event.

EOCs typically have at least one FEMA-owned and -maintained high-frequency (HF) radio for connectivity among national, regional, and state EOCs. The survivability of these HF radio units was not assessed. However, the operating band of these radios is one factor that makes them potentially vulnerable to EMP attack. Backup communications links may include satellite telephone systems and capabilities provided by amateur radio operator organizations.

EOCs also contain electronic equipment such as personal computers and digital data recorders. As with PSAPs, the capabilities supported by such equipment are vulnerable to EMP field levels as low as 3 to 6 kV/m.

Some EOCs are located below ground, which provides some protection from radiated EMP fields. However, conductive lines penetrating into these facilities must still be protected to ensure EMP survivability.

*The Emergency Alert System.* The primary method of initiating an emergency alert message involves the use of multiple commercial telecommunications lines. Therefore, the ability to provide emergency alert messages depends first on the status of the commercial telecommunications system. Broadcast of an alert message and receipt by the affected public depends on several electronic systems, including commercial radio and television stations, EAS multimodule receivers and encoders/decoders, and commercial radio and television receivers.

We performed site surveys of both a radio station and a television station. Backup power generators and spare transmitter equipment were found at both facilities. While not all commercial broadcast stations include such backup systems, the EAS has significant redundancy; some, but not all, broadcast stations are necessary for successful transmission of an emergency alert message.

We tested commonly used multimodule receiver and encoder/decoder units. The AM receiver module in its dormant mode failed at a field level of 44 kV/m. The FM receiver module exhibited erratic signal levels at 50 kV/m. No other effects were noted in testing EAS-specific equipment.

Four different television sets and two different radio receivers were tested. The vehicle testing performed for the transportation infrastructure assessment also tested radios in



vehicles. In one AM radio installed in a vehicle, a malfunction occurred at approximately 40 kV/m. All other items showed no malfunctions.

Based on these results, we expect that the EAS will be able to function in near-normal fashion following an EMP attack. The major impact that might occur is a delay in initiation and receipt of an alert message because of (1) the dependency on the commercial telecommunications system, (2) the loss of some receiver channels for the EAS equipment, (3) the potential loss of some radio and television stations from power loss or damage to transmitter components, and (4) the loss of some AM radio receivers.

**Interdependencies.** In addition to direct damage, emergency services will be degraded to the extent that they are dependent on other infrastructures that are themselves damaged by the EMP attack. Emergency services are most directly dependent on the electric power, telecommunications, transportation, and fuel infrastructures. Fire departments also are dependent on the availability of water. EMP damage to these infrastructures can seriously degrade emergency services.

Of particular importance, emergency services are heavily dependent on the ability of the Nation's PTN to process 9-1-1 calls in a timely manner. After an EMP event, the PTN is likely to experience severe delays in processing calls.<sup>12</sup> Since 9-1-1 calls are processed using the same PTN equipment as non-9-1-1 calls (until they reach special 9-1-1 call-processing equipment located in a tandem central office assigned to each PSAP), they will be subject to delays similar to those for nonemergency calls. In the short term, this will result in a large number of lost 9-1-1 calls. After several days, the operation of the PTN is expected to return to near normal, assuming no adverse effects from either extended widespread power outages or from an inability to replenish fuel supplies for backup generators. However, in the event of a widespread power outage that extends beyond the time that backup power is available or commercial power service is restored, the PTN's ability to process 9-1-1 calls will again degrade. Eventually, extended widespread power outages will result in an inability to replenish fuel supplies, essentially causing a complete loss in PTN capability to process any 9-1-1 calls.

Loss of power can also directly impact PSAP operations. In the short term, the loss of commercial power will impact local emergency services more from the standpoint of increased calls for assistance than from functional impact. Most PSAPs and EOCs have backup power generators that will allow uninterrupted operation for some time period. Long-term power outages might result in the loss of PSAPs and EOCs because of an inability to refuel the backup generators.

### Consequences

The ultimate consequences of an increased demand for emergency services and a concomitant degradation in emergency services capabilities are measured in lives lost, health impaired, and property damaged. We have no way of accurately estimating these consequences; we can only cite suggestive statistics.

*We have no accurate way to measure the impact of degraded emergency services on lives lost, health impaired, or property damaged.*

<sup>12</sup> See Chapter 3, Telecommunications.



Most importantly, we note that the lives and health of many people depend on medical technologies that, in turn, depend on electric power. People will turn to emergency services if that power is unavailable for an extended period.

Emergency medical services respond to approximately 3 million 9-1-1 calls annually for people with cardiac problems and 2.5 million others for respiratory problems.<sup>13</sup>

Fire departments responded to 1,687,500 fires in 2002. These fires resulted in property damage estimated at \$10.3 billion and 3,380 civilian deaths.<sup>14</sup> Lives and property saved by fire departments are undoubtedly also very large numbers.

Other direct consequences would result from the inability to successfully place a 9-1-1 call. Missed 9-1-1 calls can result from any number of causes, including (1) PTN outages; (2) EMP-induced damage to PSAPs, PSAP repeaters, mobile communications, or other critical support equipment; and (3) failure of commercial or residential telephone equipment.

The principal indirect consequences of a decline or collapse of emergency services are a result of a reduction in the availability of the work force. We did not attempt to quantify this effect, but note that it includes not only those directly affected, but also those who must now support those who previously would have depended on emergency services.

## Recommendations

Our recommended strategy for protection and recovery of emergency services emphasizes the establishment of technical standards for EMP protection of critical equipment and the inclusion of EMP in planning and training.

The technology for critical emergency services functions is undergoing extensive change, creating an excellent opportunity for inclusion of our recommended protection measures. This technology change is propelled in large part by the need for additional emergency services communications capability and the recognition that large-scale disasters, such as the terrorist attacks of September 11, 2001, require extensive coordination across the full spectrum of emergency services providers.

Our strategy can be realized through implementation of the following recommendations:

- ◆ DHS and state and local governments should augment existing plans and procedures to address both immediate and long-term emergency services response to EMP attack. Plans should include provisions for a protection and recovery protocol based on graceful degradation and rapid recovery that emphasizes a balance between limited hardening and provisioning of spare components. Such a plan should ensure the following:
  - The National Emergency Number Association should establish guidelines for operability and recovery of PSAPs during and after exposure to EMP.
  - The FCC should task the Network Reliability and Interoperability Council to address the NS/EP services,

◆ *Our recommended strategy for protection and recovery of emergency services emphasizes the establishment of technical standards for EMP protection of critical equipment and the inclusion of EMP in planning and training.*

<sup>13</sup> Estimates based on a survey of local PSAPs, extrapolated to the entire country.

<sup>14</sup> Statistics obtained from the National Fire Protection Association.

such as E9-1-1, and identify best practices to prevent, mitigate, and recover from an exposure to EMP.

- ◆ DHS should provide technical support, guidance, and assistance to state and local governments and federal departments and agencies to ensure the EMP survivability of critical emergency services networks and equipment. To accomplish this, the DHS should take the following actions:
  - In coordination with the Department of Energy and other relevant government entities, develop a set of EMP recovery scenarios that include coordinated attacks involving EMP and other more widely understood threats involving weapons of mass destruction.
  - In coordination with relevant government agencies, work with the appropriate standards entities (e.g., the Association of Public-Safety Communications Officials, the National Emergency Number Association, and the International Electrotechnical Commission) to establish EMP immunity standards and guidelines for critical emergency services equipment.
  - Develop training courses for emergency services providers on how to enhance immunity to, operate during, and recover from an EMP attack.
  - Develop an EMP attack consequence assessment tool to perform planning analysis and training and to assist in the identification of critical equipment and manpower requirements.
  - Establish a program to assess the vulnerability of evolving emergency services networks and electronics equipment to EMP and to develop a model plan for hardness maintenance and surveillance for implementation by state and local jurisdictions.



## Chapter 10. Space Systems

### Introduction

Over the past few years, there has been increased focus on U.S. space systems in low Earth orbits and their unique vulnerabilities, among which is their susceptibility to nuclear detonations at high altitudes—the same events that produce EMP. It is also important to include, for the protection of a satellite-based system in any orbit, its control system and ground infrastructure, including up-link and down-link facilities.

Commercial satellites support many significant services for the Federal Government, including communications, remote sensing, weather forecasting, and imaging. The national security and homeland security communities use commercial satellites for critical activities, including direct and backup communications, emergency response services, and continuity of operations during emergencies. Satellite services are important for national security and emergency preparedness telecommunications because of their ubiquity and separation from other communications infrastructures.

The Commission to Assess United States National Security Space Management and Organization conducted an assessment of space activities that support U.S. national security interests and concluded that space systems are vulnerable to a range of attacks due to their political and economic value.<sup>1</sup> Satellites in low Earth orbit generally are at risk of lifetime degradation or failure from collateral radiation effects arising from an EMP attack on ground targets.

In the course of an EMP attack, a nuclear detonation at a high altitude produces numerous other effects that can impact the performance and survival of satellites. Examination of these effects relates to the Commission's mandate in two ways. First, nuclear weapon effects on satellites can be collateral consequences of an EMP attack. Second, an EMP attack can degrade ground terminals that satellite systems require for uplinks, downlinks, and control functions.

This chapter focuses on two classes of effects that are primary threats to the physical integrity of satellites: (1) direct, line-of-sight exposure to nuclear radiation pulses (e.g., X-ray, ultraviolet, gamma-ray, and neutron pulses) and (2) chronic exposure to enhanced high-energy electrons durably trapped in the Earth's magnetic field. These effects can jeopardize satellites in orbit, as data from U.S. and Soviet high-altitude nuclear tests of 1958 and 1962 attest. **Figure 10-1** illustrates visible phenomena from several U.S. high-altitude nuclear tests. Each detonation produced copious X-ray fluxes and trapped energetic electron radiation in space. When the United States detonated the 1.4-megaton (MT) STARFISH<sup>2</sup> device on July 9, 1962, at 400 km altitude, a total of 21 satellites were in orbit or were launched in weeks following. Eight suffered radiation damage that compromised or terminated their missions.<sup>3</sup> Information concerning the fate of the remaining 13 satellites is not publicly available.

---

<sup>1</sup> Report of the Commission to Assess United States National Security Space Management and Organization, January 11, 2001.

<sup>2</sup> The high-altitude test originally known as STARFISH was not successful. A second high-altitude test called STARFISH PRIME was successfully executed at a later date to obtain the sought-after data. In much of the literature describing the damage to satellites from this test, the name of the event is called STARFISH without the PRIME modifier. For the sake of brevity we also have dropped the modifier.

<sup>3</sup> Brown, W.L., W.N. Hess, and J.A. Van Allen, "Collected Papers on the Artificial Radiation Belt From the July 9, 1962, Nuclear Detonation," *Journal of Geophysical Research* 68, 605, 1963.

In many respects, satellite electronics of the 1960s were relatively robust against nuclear effects. Their bulk and comparatively low-speed operation tended to make electronics of the era substantially less vulnerable to radiation upset and damage than modern electronics at comparable exposure levels. The discussion to follow highlights salient points of satellite vulnerabilities to nuclear explosions in the upper atmosphere or space. These vulnerabilities are considerable and incontrovertible — each worldwide fleet of satellites is at risk, but the degree of risk depends on the extent of satellite hardening, satellite location relative to the burst, resultant line-of-sight exposure to prompt radiations, and each satellite's exposure to geomagnetically trapped energetic particles of natural and nuclear origins.

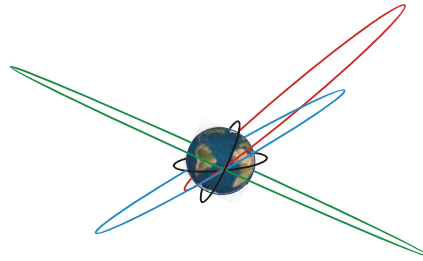


**Figure 10-1.** From left to right, the ORANGE, TEAK, KINGFISH, CHECKMATE, and STARFISH high-altitude nuclear tests conducted in 1958 and 1962 by the United States near Johnston Island in the mid-Pacific. Burst conditions for each were unique, and each produced strikingly different phenomena and different enhancements of the radiation belts.

### Terms of Reference for Satellites

Ubiquitous Earth-orbiting satellites are a mainstay of modern critical national infrastructures. Satellites provide Earth observations, communications, navigation, weather information, and other capabilities. The United States experienced significant disruption when the pager functions of PanAmSat Galaxy IV failed in May 1998.

Each satellite's orbit is optimized for its intended mission. Low Earth orbits (LEO), from 200 to 2,000 km altitude, are in proximity to the Earth and atmosphere to enable remote sensing, weather data collection, telephony, and other functions. Geosynchronous (a.k.a. geostationary) orbits (GEO) lie at about 36,000 km altitude in the equatorial plane, where their 24-hour orbital period matches the rotation of the Earth. This orbit allows GEO satellites to hover above a fixed longitude, useful for communications and monitoring of large-scale weather patterns. Satellites in highly elliptical orbits (HEO) perform specialized functions inaccessible to other orbits. For example, HEO satellites in high inclination orbits provide wide-area communications above high-latitude regions for several hours at a time. **Figure 10-2** illustrates common orbits.



**Figure 10-2. Satellite Orbits Illustrated.** Geosynchronous orbit (green) in the equatorial plane is at about 36,000 km altitude. LEO (black) are shown with inclinations relative to the equatorial plane of 30° and 90°, but any inclination is possible. A 45° inclination orbit at approximately 20,000 km altitude is shown in blue. HEO are shown in red.

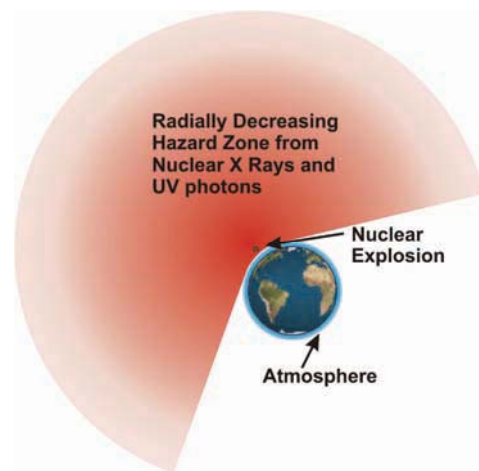
### Line-of-Sight Exposure to a Nuclear Detonation

A nuclear device will, upon detonation, radiate a portion of its total yield as X-rays, with the fraction realized a function of weapon design and attached delivery system.

Attenuation of X-rays propagating through the upper atmosphere is primarily by photoelectric absorption by oxygen and nitrogen and therefore is a function of X-ray spectrum, with higher-energy photons penetrating greater path-integrated mass density along the line of sight. Consequently, for a detonation above a (spectrally dependent) threshold altitude, X-rays emitted horizontally or upward will propagate to large distances virtually unattenuated by the atmosphere. X-rays emitted downward will be absorbed over ranges of tens of kilometers upon reaching sufficiently dense air.

Neutrons and gamma rays emitted by a detonation similarly propagate upward great distances into space for detonations above threshold altitudes. However, owing to scattering and absorption cross sections substantially smaller than X-ray photoelectric cross sections, major atmospheric attenuation of these energetic emissions occurs at altitudes below approximately 40 km.

For detonations up to a few hundred kilometers altitude, blast wave interactions between expanding weapon debris and the atmosphere may convert a majority of the kinetic yield of the weapon to ultraviolet (UV) photons. These photons propagate upward into space with little attenuation. UV photons emitted horizontally and downward are absorbed in the vicinity of the burst point to form the UV fireball. UV production for bursts above a few hundred kilometers declines rapidly, with precise values for these transition altitudes being functions of weapon output characteristics and dynamics. The combined flux of energetic photons (X-ray, gamma, and UV) and neutrons irradiates a vast region of space, diminished by spherical divergence, as shown in **figure 10-3**. The actual size of the hazard zone depends on weapon yield, detonation altitude, and the degree of satellite hardening against disruption or harm. Damage to satellite structures and to coatings on solar panels and sensor optics occurs when X-ray and UV fluxes exceed critical thresholds. Electronics damage similarly ensues when X-ray and gamma pulses induce destructive electric currents in circuit elements and when energetic neutrons penetrate solid-state circuitry.



**Figure 10-3. Areas of Space Irradiated by Photons and Neutrons.** Where not shadowed by the Earth or shielded by atmospheric attenuation, X-rays and UV photons travel great distances from a high-altitude nuclear detonation where they may inflict damage to satellites.



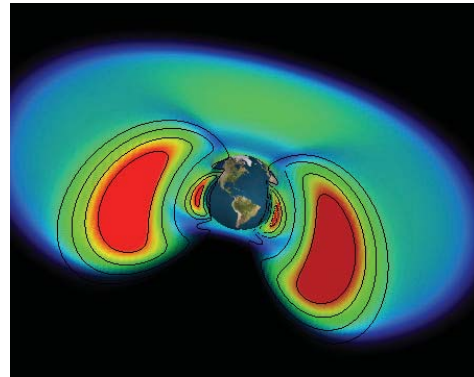
## Persistently Trapped Radiation and Its Effects

In 1957, N. Christofilos at the University of California Lawrence Radiation Laboratory postulated that the Earth's magnetic field could act as a container to trap energetic electrons liberated by a high-altitude nuclear explosion to form a radiation belt that would encircle the Earth.<sup>4</sup> In 1958, J. Van Allen and colleagues at the State University of Iowa used data from the Explorer I and III satellites to discover the Earth's natural radiation belts.<sup>5</sup> **Figure 10-4** provides an idealized view of the Van Allen belts. Later in 1958, the United States conducted three low-yield ARGUS high-altitude nuclear tests, producing nuclear radiation belts detected by the Explorer IV satellite and other probes. In 1962, larger tests by the United States and the Soviet Union produced more pronounced and longer lasting radiation belts that caused deleterious effects to satellites then in orbit or launched soon thereafter.

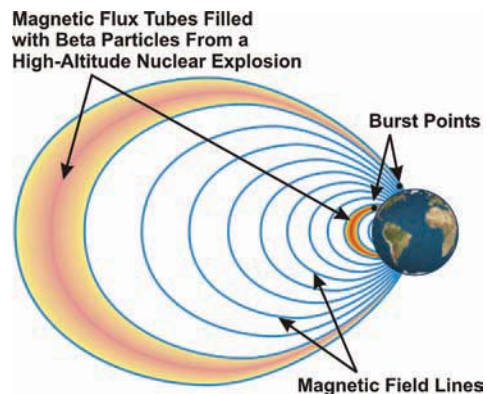
A nuclear detonation is a significant source of free electrons originating from the highly ionized plasma that is a product of the nuclear blast. Nuclear detonations also create trapped radiation by beta decay of radioactive weapon debris and free-space decay of neutrons from the explosion, thereby creating electrons with energies up to several million electron volts (MeV). The most notable tests producing radiation hazards to satellites were the U.S. STARFISH detonation and three high-altitude tests by the Soviets, all conducted in 1962.

One assesses natural and trapped nuclear radiation effects on contemporary satellites by calculating repeated passage of a satellite through radiation belts over the satellite's lifetime. While the geometry of a satellite's orbit is relatively straightforward, characterization of spatial and temporal properties of both natural and nuclear radiation belts is a complex problem. Nevertheless, one can establish relative scaling of levels of vulnerability from radiation belt geometry, as shown in **figure 10-5**. Intensities of radiation belts depend strongly on burst latitude. A burst at low latitude fills a small magnetic flux tube volume, so trapped flux tends to be concentrated and intense. The same burst at higher latitude fills a much larger magnetic flux tube volume.

All quantitative assessments of effects on satellite lifetime provided in this chapter are based on calculations carried out using a code that tracks the satellite orbits through space and calculates the accumulated radiation dose.



**Figure 10-4.** Naturally occurring belts (Van Allen belts) of energetic particles persistently trapped in the geomagnetic field are illustrated.



**Figure 10-5.** Schematic diagram of relative intensities of trapped fluxes from two identical high-altitude nuclear detonations.

<sup>4</sup> Christofilos, N.C., Proceedings of the National Academy of Sciences, U.S. 45, 000, 1959.

<sup>5</sup> Van Allen, J.A., and L.A. Frank, "Radiation Around the Earth to a Radial Distance of 107,400 km," *Nature*, 183, 430, 1959.

## **Nuclear Weapon Effects on Electronic Systems**

Electronic systems perform many critical spacecraft functions. An electronic power control system regulates the energy obtained from the solar cells. Attitude control circuits keep the vehicle oriented so that solar panels receive maximum exposure to the sun and sensors face the Earth. Information collected by sensors must be processed, stored, and transmitted to the Earth on demand. Communications satellites receive information, possibly process it, and then retransmit it, all by electronic circuits. Both prompt and long-term radiation effects have the potential for corrupting these functions in systems that lack hardening or other mitigation of nuclear effects.

### ***Total-Dose Damage***

A common criterion for failure of an electronic part is the total radiation energy per unit volume deposited in silicon. This absorbed energy density is expressed in rads(Si) (1 rad = 100 ergs/gram). Natural radiation to an electronic part in the International Space Station (ISS) behind a 2.54 mm semi-infinite (very large) aluminum slab averages about 100 rads per year. Previous literature has commonly used this shielding thickness for satellite radiation exposure calculations. However, it should be noted that electronics are placed in a variety of locations in a satellite and, therefore, can have different levels of shielding. Natural radiation to an electronic part in LEO, such as the National Oceanic and Atmospheric Administration (NOAA) satellite, in polar orbit behind a 2.54 mm semi-infinite aluminum slab is, on long-term average, about 620 rads per year, while some satellites with the same shielding might receive 50 kilorads per year.<sup>6</sup> Electronics must be shielded in accordance with the intended orbit to limit the dose received to a tolerable level.

### ***Radiation-Induced Electrostatic Discharge***

One hazard to spacecraft passing through the natural or nuclear radiation belts is internal or “deep dielectric” charging.<sup>7</sup> Lower-energy electrons (40 to 300 keV) become embedded in surface materials or poorly shielded internal materials and, on a timescale of hours to days, can build up sufficient electric field to cause a discharge, often resulting in satellite upset and occasionally in serious damage. Thermal blankets, external cables, and poorly shielded circuit boards are prime candidates for this type of charging. Modern coverglasses and optical solar reflectors are made sufficiently conductive to avoid such local charge buildup.

### ***Radiation Effects Assessment and Hardening***

Susceptibility of electronic components to nuclear weapon radiation has been studied intensively both experimentally and analytically since 1956. State-of-the-art computers and algorithms are used to extrapolate the experimental results to an operational environment.

The EMP Commission’s mission was to evaluate the threat of high altitude nuclear weapon-induced EMP on American national infrastructure. A collateral result of a high altitude burst is a radiation threat to satellites, primarily those residing in LEO. The damage manifests as upset or burnout of sensitive microelectronics on the spacecraft. In some

---

<sup>6</sup> Schreiber, H., “Space Environments Analyst, Version 1.2,” 1998 Space Electronics, Inc., Calculations using Space Radiation 4.0, Space Radiation Associates, Eugene, OR, 1998.

<sup>7</sup> Frederickson, A.R., “Radiation-Induced Dielectric Charging in Space Systems and Their Interactions with Earth’s Space Environment,” eds. H.B. Garrett and C.P. Pike, Progress in Astronautics and Aeronautics, vol. 71, AIAA, 1980.

cases, damage can occur to external surfaces and structural members, as well as to optical components and to solar-cell power sources.

To address these issues, we considered a plausible set of 21 EMP nuclear events, which are listed in **table 10-1**. These disparate threats were then imposed upon a set of satellites (**table 10-2**) representative of the U.S. space infrastructure to examine the ancillary effects of an exoatmospheric nuclear detonation.

The time frame of interest is through the year 2015. As indicated in **table 10-1**, cases include both higher and lower yield weapons. Though not included in **tables 10-1** through **10-6**, each event is also associated with a particular latitude and longitude.

**Table 10-1. Trial Nuclear Events**

Event	Yield (kT)	Height of Burst (km)	L-Value <sup>8</sup>
1	20	200	1.26
2	100	175	1.09
3	300	155	1.09
4	10	300	1.19
5	100	170	1.16
6	800	368	1.27
7	800	491	1.36
8	4,500	102	1.11
9	4,500	248	1.16
10	30	500	1.23
11	100	200	1.18
12	20	150	1.24
13	100	120	1.26
14	500	120	1.26
15	100	200	1.03
16	500	200	1.03
17	5,000	200	1.03
18	1,000	300	4.11
19	10,000	90	4.19
20	1,000	350	6.85
21	10,000	90	6.47

While the primary threat from nuclear-pumped radiation belts is to satellites in relatively low orbits, high-yield bursts could be detonated at latitudes and longitudes that would threaten higher orbiting satellites (Events 18 to 21). These bursts would be at relatively high latitudes sufficient to allow high-energy electrons to migrate along geomagnetic field lines that reach the high altitudes at which geosynchronous satellites reside.<sup>9</sup> Of course, at higher orbital altitudes, the density of ionizing radiation would be much reduced over that experienced by a satellite orbiting at lower altitudes and

<sup>8</sup> It is conventional (and useful) to describe the magnetic field lines on which electrons are trapped as belonging to numbered L-shells. The L-value of a field line is the distance (in Earth radii measured from the location of Earth's dipole field source) at which the field line intersects the magnetic equator. The inner belt peaks around L = 1.3, and the outer belt, near L = 4. Trapped electrons rapidly gyrate about the field lines, bounce along the field lines between mirror points, and drift around the Earth.

<sup>9</sup> As illustrated in **figure 10-5**, magnetic field lines that intersect the Earth at high northern and southern latitudes extend outward into space to relatively large distances. Conversely, magnetic field lines that intersect the Earth at low latitudes extend relatively short distances into space. Consequently, geomagnetically trapped electrons created by detonations at high latitudes can propagate along field lines out to very high altitudes where satellites orbit, whereas trapped electrons created by low-latitude bursts would be less likely to do so.

subjected to the same nuclear source due to the much larger volume in which the ionizing energy is distributed.

**Table 10-2. Analysis of Satellites**

Satellite	Altitude (km)	Mission
NOAA/DMSP	800 (LEO)	Weather, remote sensing, search and rescue
TERRA/IKONOS	700 (LEO)	Moderate-high resolution imaging Earth resources and Earth sciences High resolution imagery, digital photography
ISS	322 (LEO)	Space science and technology
Generic GEO	GEO	Remote sensing
Generic HEO	HEO	Launch detection and other

It is emphasized that these events were chosen only for purposes of effects analysis. The satellites (**table 10-2**) were chosen to be representative of the many types and missions in orbit and to be representative targets for the radiation effects.

### **Prompt Radiation Effects**

When a weapon is detonated at high altitude, satellites that lie within line of sight of the burst will be subject to direct (X-ray) radiation. Satellites in the shadow cast by the Earth will not be directly irradiated, as illustrated in **figure 10-3**, but will be subject to electron radiation as they transit debris and decay-products (primarily energetic beta electrons) mentioned previously that are trapped in the Earth's magnetic field. If there is a significant mass of intervening atmosphere between the detonation point and the satellite, direct nuclear radiation will be attenuated. Lacking this intervening shield, the radiation fluence will decrease as the inverse square of the distance.

Worst-case situations occur when a satellite is nearest the burst; for example, directly above or below it. In such cases, the range between satellite and burst is minimized, and X-ray, gamma, and neutron fluences on the satellite are maximized. Full evaluation of this hazard requires statistical analysis. The likelihood that the satellite will be in direct line of sight of the burst is typically 5 to 20 percent, depending on orbital parameters for the satellite and burst location. Even then, damage may be ameliorated by either distance or intervening atmosphere.

Calculations of X-ray exposure probabilities were performed for Events 9, 13, 17, and 18. The calculations yield the probability that a specific satellite will be exposed to a specified level of X-ray fluence. Results appear in **table 10-3**. With this information, one can estimate the probability of satellite damage based on known damage thresholds for spacecraft materials. Thresholds for various types of damage were chosen at, or close to, values accepted by the engineering community. Here, thermomechanical damage refers to removal or degradation of the coatings on solar cell surfaces. Depending on nuclear weapon output spectra, coating damage is generally a satellite's most sensitive thermomechanical damage mode. SGEMP (System-Generated EMP) burnout is damage caused by currents associated with X-ray-induced electron emission. Latch-up is a logic state setting of a semiconductor device that becomes frozen as a result of radiation exposure. Latch-up may cause large currents to flow in the affected circuit, resulting in unacceptable current-induced damage (i.e., burnout).

Line-of-sight exposure of the ISS to photons can cause significant damage to the solar-array coverglass coatings for Events 6, 7, 8, 9, and 17. NOAA/DMSP and TERRA/IKONOS are unlikely to be promptly affected thermomechanically by a line-of-sight

photon exposure in any of our postulated nuclear events. Satellites in GEO are sufficiently far away because of their higher altitudes that the inverse square fall-off of the radiation reduces the potential exposure to a tolerable level.

**Table 10-3. Probability That Satellites Suffer Damage by Direct Exposure to X-Rays**

Satellite	Event	Probability of damage due to thermomechanical damage (%)	Probability of damage due to SGEMP/burnout (%)	Probability of damage due to latch-up/burnout (%)
ISS	9	1.7	4	4.2
	18	0	5	5
	13	~ 0	3	4
	17	1.7	5	5
NOAA	18	0.2	19	20
	13	0	3	5
	17	1	7	8
TERRA	18	~ 0.3	18	18
	13	0	2	5
	17	1.2	7	7

### ***Permanent Damage from Exposure to the Enhanced Electron Belts***

For this report, nuclear-enhanced electron belts are modeled as though they were providing a relatively constant trapped-electron environment. **Tables 10-4, 10-5, and 10-6** display reduced lifetimes of satellites that result from 17 of the 21 events. Results of events 18 through 21 will be discussed below.

**Table 10-4. Trial Events in Group 1**

Event	Yield (kT)	HOB (km)	Time to Failure (days)		
			NOAA	TERRA	ISS
1	20	200	30	70	150
2	100	175	15	30	50
3	300	155	4	7	9
4	10	300	20	60	5,400
5	100	170	30	70	100

Reduction in satellite lifetime is based on total dose from higher energy electrons to internal electronics, assumed to be shielded by a 0.100-inch slab of aluminum. In evaluating the biological response of astronauts to radiation on the ISS, 0.220 inches of slab shielding was assumed because the astronauts would usually be inside the pressurized modules of the space station. Some critical electronics for the station were still assumed to be shielded by only 100 mils of aluminum. Satellites are assumed to be hardened to twice the long-term-average natural background radiation encountered during a nominal mission.<sup>10</sup> Just as with photons, damage to spacecraft thermal, optical, and other surface coatings is caused by exposure to electrons of relatively low energies.

Except for the ISS in Event 4, even the low-yield events are capable of imposing a much-reduced lifetime on the satellites.

In the set of events depicted in **table 10-5**, the large weapon used in Event 17 inflicts severe damage on the ISS. Significantly, this exposure would cause radiation sickness to the astronauts within approximately 1 hour and a 90 percent probability of death within 2 to 3 hours.

<sup>10</sup> While the use of twice the expected long-term-average exposure as a gauge of lifetime, as discussed here, is common practice, it relies entirely on total dose as a measure of radiation tolerance and ignores dose rate effects. Risks from circumstances involving nuclear detonations, where dose rates could be much larger than encountered under natural conditions, may be underestimated.



Events 6 through 11 (**table 10-6**) were chosen within a geographical region where satellites could be placed at risk from a direct EMP attack resulting from regional contingencies.

**Table 10-5. Trial Events in Group 2**

Event	Yield (kT)	HOB (km)	Time to Failure (days)		
			NOAA	TERRA	ISS
12	20	150	25	60	230
13	100	120	60	200	200
14	500	120	4	6	3
15	100	200	10	20	30
16	500	200	1	3	4
17	5,000	200	0.1	0.1	0.1

**Table 10-6. Trial Events in Group 3**

Event	Yield (kT)	HOB (km)	Time to Failure (days)		
			NOAA	TERRA	ISS
6	800	368	1	1	0.5
7	800	491	1	1	1
8	4,500	102	0.1	0.2	0.2
9	4,500	248	0.1	0.2	0.2
10	30	500	40	100	150
11	100	200	10	17	20

The results of weapons detonated at high latitudes (Events 18 through 21) produced no dramatic nuclear effects. This is largely because these satellites are designed to operate in a far more hostile natural space environment due to the solar wind than are those in LEO.

Generally, most papers dealing with satellite lifetimes following a high-altitude nuclear detonation treat radiation effects on newly launched satellites with no pre-burst accumulated total dose. Except for satellites launched as replacements after a detonation, a more realistic assessment would assume a high-altitude detonation after a satellite had been in orbit for a portion of its anticipated service life. If a satellite is near the end of its design lifetime (i.e., has accumulated the majority of the total dose it can tolerate) prior to the detonation, the dose absorbed from a nuclear-pumped belt could cause prompt demise. To evaluate potential life-shortening effects on satellites, we examined a constellation of generic satellite systems. To assess sensitivity to assumed hardening level, we evaluated two hypothetical constellations. One constellation was assumed hardened to 1.5 times the natural total dose anticipated over the design lifetime (1.5x). The other constellation was assumed hardened to 2x. The scenario involved a 10 MT burst (50 percent fission yield) detonated on May 23, 2003, at an altitude of 90 km over northern Lake Superior (48.5 degrees north latitude, 87 degrees west longitude). Total dose for each constellation was based on realistic code calculations.

**Figure 10-6** shows the resulting number of satellites remaining as a function of time after the burst. The blue and red curves correspond to the constellations hardened to 1.5x and 2x, respectively. Corresponding outage times for ground-based receivers are shown in **Figure 10-7**. Clearly, decreasing satellite hardening by 25 percent has a marked effect on survivability in this case.



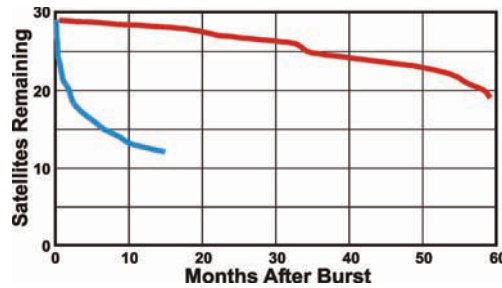


Figure 10-6 . Satellites remaining after a 10 MT burst over Lake Superior



Figure 10-7. Satellite ground-based receiver outage time after a 10 MT burst over Lake Superior

HEO satellites already reside in orbits that are relatively challenging in terms of the natural radiation environment. Assuming these satellites are hardened to twice the natural dose they would normally accumulate in 15 years, a satellite's electronics would be hardened to approximately 325 krad behind a 100 mil (0.1 inch) semi-infinite slab of aluminum. With this level of hardness, one would expect that these satellites would not be vulnerable to a high-altitude burst of a single, low-yield (approximately 50 kT) device of unsophisticated design. Realistic code calculations suggest this is indeed the case.

Three large-yield events were investigated to determine whether they would present a threat to HEO satellites. Two of these events (Events 11 and 21) would not present a total ionizing dose problem for the satellite. Although Event 21 is a 10-MT burst, it has little effect on a HEO satellite because the trapped electrons are spread out over a large L-shell region. In contrast, the 100 kT of Event 11 does result in some detectable radiation accumulation on the satellite as it passes through altitudes near perigee. The yield is, however, too low to present a threat to the satellite. A 5-MT burst depicted in Event 17, on the other hand, does present a substantial threat to HEO satellites, given the hardening assumptions mentioned earlier. **Figure 10-8** shows that the assumed 2x natural hardening level of the satellite is exceeded about 36 days after Event 17.

Analysis of direct EMP attacks over the northern continental United States (CONUS) or Canada indicates lesser risk to LEO satellites from weapons with yields ranging from 10 kT to 100 kT. For yields approaching 1 MT (or greater) detonated at such latitudes, it becomes more difficult to predict the fate of LEO satellites. The larger yields make more severe nuclear-enhanced trapped flux environments, but depletion rates of trapped fluxes (both natural and nuclear) are difficult to predict.

### Satellite Ground Stations

Although bursts over CONUS may not directly damage satellites, the EMP effect on ground control stations could still render some satellites inoperable. We have focused our analyses on collateral weapon effects on satellites, without discussion of EMP effects on ground stations used for uplinks, downlinks, and satellite control. Currently, many of the

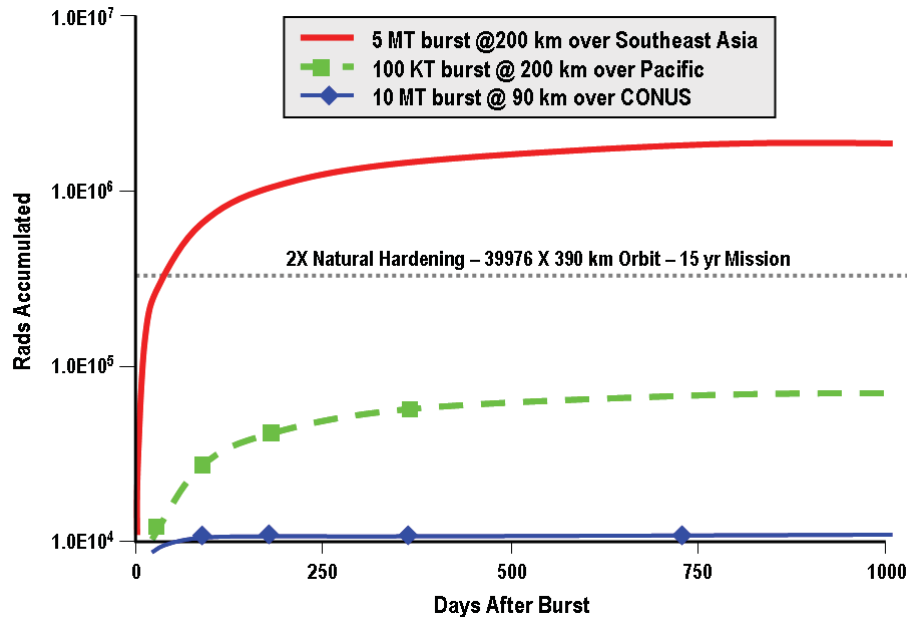


Figure 10-8. HEO satellite exposure to trapped radiation produced by Events 11, 17, and 21

important satellite systems use unique transmission protocols with dedicated ground terminals. Unique protocols limit interoperability, so loss of dedicated ground terminals could readily compromise overall functionality of a system, even if the system's satellites remained undamaged.

While satellites generally are designed to operate autonomously, with periodic house-keeping status downloads to ground controllers and uploads of commands, once damaged, satellites may require frequent, perhaps continuous, control from the ground to remain even partially functional. Thus, loss of ground stations to EMP could render otherwise functional satellites ineffective or lead to premature loss.

A comprehensive analysis of overall satellite system degradation should include potential loss of ground stations and cost/benefit trade-offs with respect to EMP hardening. A scenario-based analysis would reveal the extent to which loss of individual ground stations may pose an additional level of vulnerability.

## Discussion of Results

Given inherent satellite fragility owing to severe weight constraints, any nation with missile lift capability and sufficient technology in the requisite disciplines can directly attack and destroy a satellite. Such attacks are outside the focus of this study. The Commission considered only hazards to satellites that may arise as collateral nuclear weapon effects during an EMP attack. The prominent collateral hazards are prompt nuclear output (X-rays, gamma rays, and neutrons), high fluences of UV photons generated by some high-altitude nuclear detonations, and nuclear burst enhancement (pumping) of the radiation belts surrounding the Earth in the region of space where satellites orbit.

The worst-case exposure of a satellite to direct x-radiation from a nuclear weapon can be lethal. For LEO satellites, the threat can be nonnegligible, but for satellites at GEO, the large distance between a detonation designed for an EMP attack and a satellite makes the probability of direct damage very low. The same argument holds for exposure to gamma rays, neutrons, and burst-generated UV light.

Nuclear-enhanced radiation belts must be considered differently, owing to their persistence and wide spatial distribution around the Earth. Because the natural trapped radiation environment at GEO is more severe on average than at most LEO locations, satellites at GEO typically are hardened to a greater extent than LEO satellites. Absent large yields (megatons), burst-generated energetic electron fluxes trapped in high-latitude (i.e., high L-shell) magnetic flux tubes generally are not sufficiently intense and long-lasting to cause the early demise of satellites in GEO, unless those satellites have accumulated sufficient natural radiation exposure to put them near the end of their service lives.<sup>11</sup>

Satellites in LEO are much more susceptible to damage from both direct and persistent radiation that results from an EMP attack, but the possibility of damage is highly dependent on weapon parameters (latitude and longitude, height of burst [HOB], and weapon yield).

Line-of-sight exposure of LEO research satellites such as ISS to X-ray and UV photons can cause significant damage to solar-array coverglass coatings for Events 6, 8, 9, 17, and 19. While such exposures are statistically infrequent, in those instances where they occur, they will result in immediate loss of many operational capabilities, as well as loss of power generating capacity.

The low-energy component of trapped-electron flux from beta decay of fission products and decay of free neutrons exceeds the long-term average natural flux for the high-yield Events 8, 9, and 17. Such flux levels will cause electrostatic breakdown in certain types of thermal radiator coatings and external cables on NOAA and TERRA within the first few days following the burst.

### ***Uncertainties in Estimates***

Uncertainties in satellite vulnerabilities result from imprecise knowledge of threat environments, combined with uncertainties in responses of satellite materials to those environments. Difficulties in characterizing aging effects of materials exposed to on-orbit conditions for extended periods exacerbate these uncertainties.

In the following comments, it is assumed that the weapons in question mirror U.S. technology available in the time frame 1970 to 1980.

Uncertainties in direct line-of-sight exposure of a satellite to radiation from a nuclear detonation result primarily from unknowns associated with the design of an offensive weapon, its delivery system, and its detonation altitude. These factors determine the fraction of weapon yield emitted as photons, neutrons, and beta particles and, hence, the type and magnitude of damage they inflict on satellites. Variability of weapon designs is estimated to lead to an uncertainty of approximately plus or minus a factor of five in UV hazard source strength (radiation primarily emitted from a weapon's case and its packaging within a delivery vehicle [but see below for more on UV photons]). Based on computational correlations with experimental data, there exists at least a factor of 10 uncertainty in X-ray spectral intensity at arbitrary photon energies of a kilovolt or more. Uncertainties in gamma-ray fluence and flux predictions are thought to be on the order of  $\pm 15$  percent, as are those for prompt neutrons. Total yield is believed to be accurate to  $\pm 10$  percent.

---

<sup>11</sup> The reader is reminded that our analysis deals only with collateral damage resulting from an EMP attack. Direct attack on satellites at any altitude, though serious, is not within the bounds of this analysis.

For bursts below a few hundred kilometers altitude, the debris-air blast-wave-generated fluence of UV photons (which can be as large as 80 percent of the kinetic yield of the device) carries an estimated uncertainty factor of 3 to 10, depending primarily on device characteristics. These uncertainty factors are ameliorated to some degree by decreasing burst altitude. Detonations below approximately 90 km occur in sufficiently dense air that UV photons are largely absorbed before they can escape to space.

Uncertainties in trapped radiation environments from high-altitude nuclear detonations also result from unknowns in offensive weapon design, but additional uncertainties arise in dispersal of radioactive weapon debris, efficiency with which beta particles become trapped in the geomagnetic field, subsequent transport of trapped particles, and the rapidity with which nuclear-burst enhancements of the radiation belts decay into the natural background. Under the best of circumstances, uncertainties in the intensity and persistence of trapped radiation estimated for the events considered in this report are at least a factor of 10 and are likely substantially more in situations that depart from limited circumstances of past nuclear tests.

## Findings

### ***Potential Vulnerabilities***

An EMP attack on any of several important geographic regions could cause serious damage to LEO satellites. The STARFISH high-altitude nuclear burst greatly enhanced the high-energy electron environment in LEO, resulting in the early demise of several satellites on orbit at the time.<sup>12</sup> Copious documentation exists that describes recent radiation-induced satellite failures due to the natural radiation environment alone.

Given the large uncertainties discussed above, there may be a temptation to ignore the issue of high-altitude nuclear threats to satellites for the time being simply because insufficient information is available to implement a cost-effective protection solution. We believe that ignoring the issue would be ill advised for a number of reasons, including the consequences of losing possibly tens of billions of dollars in LEO space assets in a short time.

### ***Mitigation of Threats***

Any adversary possessing a lift and orbiting control capability can destroy a satellite: it is clearly neither cost effective nor desirable to harden every satellite against every possible threat. The challenge is to weigh risks/rewards of mitigation against mission priorities and plausible threats. A number of threat mitigation measures exist or have been proposed as an alternative or supplement to hardening.

Any combination of hardening and mitigation options can be chosen to achieve the required degree of survivability. Alternatives must be explored, documented, and reviewed so that management and users of space assets can make rational appraisals of the costs, benefits, and consequences of space system degradation and/or loss.

### ***Hardening of Satellites and Ground Stations***

Commercial satellites are hardened against their natural orbital environment to achieve the lifetime necessary to realize a profit. The technology to accomplish this goal is built into their design and factored into their cost. Protection from nuclear threats is not

---

<sup>12</sup> Weenas, E.P., "Spacecraft Charging Effects on Satellites Following STARFISH Event," RE-78-2044-057, February 17, 1978.

provided to commercial satellites because, from the commercial operator's perspective, it is not cost effective to do so.

The cost of hardening a system has been a subject of continuing controversy for the past 45 years. Systems project offices tend to estimate high to avoid the introduction of measures that threaten to escalate system cost. Achievable cost control is contingent upon ab initio design of radiation hardness into the system rather than on retrofitting it. Options other than hardening and shielding include repositioning selected satellites in times of stress to minimize exposure to enhanced radiation belts.

If the ground stations for satellites in any orbit are not hardened to EMP, the utility of the satellites could degrade, depending on their ability to operate autonomously.

### **Recommendations**

- ◆ Each Federal Government organization that acquires and/or uses space should execute a systematic assessment of the significance of each such space system, particularly those in low Earth orbits, to its missions. Information from this assessment and associated cost and risk judgments will inform senior government decision-making regarding protection and performance assurance of these systems, so that each mission can be executed with the required degree of surety in the face of possible threats.

## Chapter 11. Government

### Introduction

A primary role of the Federal Government is to defend the Nation against threats to its security. EMP represents one such threat. Indeed, it is one of a small number of threats that can hold our society at risk of catastrophic consequences. The Executive branch of the Federal Government bears the responsibility for executing a strategy for dealing with this threat. The Commission has recommended a strategy for addressing this threat that combines prevention, protection, and recovery. It represents what we believe to be the best approach for addressing the EMP threat.

The Commission has identified an array of recommendations relating to civilian infrastructures that are logical outgrowths of our recommended strategy. Those recommendations relating to civilian infrastructures are contained in the individual chapters of this volume and will not be repeated here. Implementation of these recommendations will result in the identification of responsibilities at the regional, state, and local levels.

The Federal Government not only has the responsibility for being appropriately postured to cope with all aspects of the EMP threat, including preparations for recovery, but also has the responsibility to be able to respond to and manage national recovery in a competent and effective manner in the wake of an EMP attack. American citizens expect such competence and effectiveness from responsible government officials at all levels. In order to properly manage response and recovery, essential government functions will have to survive and function in the wake of an EMP attack.

### Maintaining Government Connectivity and Coherence

It is essential that the Government continues to function through an electromagnetic pulse (EMP) emergency. Events over the last few years have highlighted the need for assured and real-time communications connectivity between government leadership and organizational assets for both crisis management and the management of a controlled recovery. Plans to ensure the continued functioning of government are embodied in Continuity of Operations (COOP) plans prepared by government organizations in anticipation of emergency situations and Continuity of Government (COG) planning to ensure the survival of constitutional government. National Security Presidential Directive 51 (NSPD 51) and Homeland Security Presidential Directive 20 (HSPD 20 on the subject of “National Continuity Policy”, as described in a White House summary released May 9, 2007<sup>1</sup>), outlines these issues and directs the implementation of COOP and COG (excerpts noted below). The EMP Commission met with National Security Council staff to discuss COG-related issues as they might relate to EMP threats. However, COG planning remains highly classified, and only this top-level overview can be provided within this venue.

### Recommendations

- ◆ The Department of Homeland Security (DHS) should give priority to measures that ensure the President and other senior Federal officials can exercise informed leadership of the Nation in the aftermath of an EMP attack and that improve post-attack response capabilities at all levels of government.

---

<sup>1</sup> National Security and Homeland Security Presidential Directive,  
<http://www.whitehouse.gov/news/releases/2007/05/20070509-12.html>.



- ◆ The President, Secretary of Homeland Security, and other senior officials must be able to manage national recovery in an informed and reliable manner. Current national capabilities were developed for Cold War scenarios in which it was imperative that the President have assured connectivity to strategic retaliatory forces. While this requirement is still important, there is a new need for considerably broader and robust connectivity between national leaders, government at all levels, and key organizations within each infrastructure sector so that the status of infrastructures can be assessed in a reliable and comprehensive manner and their recovery and reconstitution can be managed intelligently. The DHS, working through the Homeland Security Council, should give high priority to identifying and achieving the minimum level of robust connectivity needed for recovery following an EMP attack. In doing so, DHS should give particular emphasis to exercises that evaluate the robustness of the solutions being implemented.
- ◆ Working with state authorities and private sector organizations, the DHS should develop draft protocols for implementation by emergency and other government responses following an EMP attack, Red Team these extensively, and then institutionalize validated protocols through issuance of standards, training, and exercises.

***NSPD 51/HSPD 20***  
***Subject: "National Continuity Policy"***  
***9 May 2007***

**Purpose**

(1) This directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies. This policy establishes "National Essential Functions," prescribes continuity requirements for all executive departments and agencies, and provides guidance for State, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

**Definitions**

(2) In this directive:

(a) "Category" refers to the categories of executive departments and agencies listed in Annex A to this directive;

(b) "Catastrophic Emergency" means any incident, regardless of location, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the U.S. population, infrastructure, environment, economy, or government functions;

(c) "Continuity of Government," or "COG," means a coordinated effort within the Federal Government's executive branch to ensure that National Essential Functions continue to be performed during a Catastrophic Emergency;

(d) "Continuity of Operations," or "COOP," means an effort within individual executive departments and agencies to ensure that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies;

(e) "Enduring Constitutional Government," or "ECG," means a cooperative effort among the executive, legislative, and judicial branches of the Federal Government, coordinated by the President, as a matter of comity with respect to the legislative and judicial branches and with proper respect for the constitutional separation of powers among the branches, to preserve the constitutional framework under which the Nation is governed and the capability of all three branches of government to execute constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, and interoperability and support of the National Essential Functions during a catastrophic emergency;

(f) "Executive Departments and Agencies" means the executive departments enumerated in 5 U.S.C. 101, independent establishments as defined by 5 U.S.C. 104(1), Government corporations as defined by 5 U.S.C. 103(1), and the United States Postal Service;

(g) "Government Functions" means the collective functions of the heads of executive departments and agencies as defined by statute, regulation, presidential direction, or other legal authority, and the functions of the legislative and judicial branches;

(h) "National Essential Functions," or "NEFs," means that subset of Government Functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP and COG capabilities; and

(i) "Primary Mission Essential Functions," or "PMEFs," means those Government Functions that must be performed in order to support or implement the performance of NEFs before, during, and in the aftermath of an emergency.

**Policy**

(3) It is the policy of the United States to maintain a comprehensive and effective continuity capability composed of Continuity of Operations and Continuity of Government programs in order to ensure the preservation of our form of government under the Constitution and the continuing performance of National Essential Functions under all conditions.

**Implementation Actions**

(4) Continuity requirements shall be incorporated into daily operations of all executive departments and agencies. As a result of the asymmetric threat environment, adequate warning of potential emergencies that could pose a significant risk to the homeland might not be available, and therefore all continuity planning shall be based on the assumption that no such warning will be received. Emphasis will be placed upon geographic dispersion of leadership, staff, and infrastructure in order to increase survivability and maintain uninterrupted Government Functions. Risk management principles shall be applied to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences.

...

(10) Federal Government COOP, COG, and ECG plans and operations shall be appropriately integrated with the emergency plans and capabilities of State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to promote interoperability and to prevent redundancies and conflicting lines of authority. The Secretary of Homeland Security shall coordinate the integration of Federal continuity plans and operations with State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to provide for the delivery of essential services during an emergency.

(11) Continuity requirements for the Executive Office of the President (EOP) and executive departments and agencies shall include the following:

(a) The continuation of the performance of PMEFS during any emergency must be for a period up to 30 days or until normal operations can be resumed, and the capability to be fully operational at alternate sites as soon as possible after the occurrence of an emergency, but not later than 12 hours after COOP activation;

(b) Succession orders and pre-planned devolution of authorities that ensure the emergency delegation of authority must be planned and documented in advance in accordance with applicable law;

(c) Vital resources, facilities, and records must be safeguarded, and official access to them must be provided;

(d) Provision must be made for the acquisition of the resources necessary for continuity operations on an emergency basis;

(e) Provision must be made for the availability and redundancy of critical communications capabilities at alternate sites in order to support connectivity between and among key government leadership, internal elements, other executive departments and agencies, critical partners, and the public;

(f) Provision must be made for reconstitution capabilities that allow for recovery from a catastrophic emergency and resumption of normal operations; and

(g) Provision must be made for the identification, training, and preparedness of personnel capable of relocating to alternate facilities to support the continuation of the performance of PMEFS.

...

(19) Heads of executive departments and agencies shall execute their respective department or agency COOP plans in response to a localized emergency and shall:

(a) Appoint a senior accountable official, at the Assistant Secretary level, as the Continuity Coordinator for the department or agency;

(b) Identify and submit to the National Continuity Coordinator the list of PMEFS for the department or agency and develop continuity plans in support of the NEFs and the continuation of essential functions under all conditions;

(c) Plan, program, and budget for continuity capabilities consistent with this directive;

(d) Plan, conduct, and support annual tests and training, in consultation with the Secretary of Homeland Security, in order to evaluate program readiness and ensure adequacy and viability of continuity plans and communications systems; and

(e) Support other continuity requirements, as assigned by category, in accordance with the nature and characteristics of its national security roles and responsibilities

...

GEORGE W. BUSH

## Chapter 12. Keeping The Citizenry Informed: Effects On People

### Introduction

The best current estimate is that the electromagnetic pulse (EMP) produced by a high-altitude nuclear detonation is not likely to have direct adverse effects on people. Such effects have not been observed for the personnel who operate EMP simulators.<sup>1</sup> Medical surveillance studies on human exposure to pulsed electromagnetic fields have supported this inference.<sup>2</sup>

An important exception is people whose well-being depends on electronic life support equipment. They will be directly impacted by effects that disrupt or damage such devices. Research sponsored by the Commission suggests that some heart pacemakers may be among the devices susceptible to upset from high-altitude EMP.<sup>3,4</sup>

While most effects on people would be indirect, they could be significant in a just-in-time economy in which local stocks of medicines, baby food, and other health-critical items are limited. The physical consequences of the serious high-altitude EMP attacks on the United States (U.S.) of concern to the Commission would likely include the failure of the electric power grid and degradation of telecommunication systems, computers, and electronic components over large areas of the country. A disruption of this scale could cripple critical infrastructures and hinder the delivery of day-to-day necessities, because of the interconnectivity of telecommunication networks and the electrical dependence of most cities, government agencies, businesses, households, and individuals. It also could require a long recovery period. To assess human consequences, the contingency of concern is one in which electricity, telecommunications, and electronics are out of service over a significant area for an extended period of time.

The human consequences of such a scenario include the social and psychological reactions to a sudden loss of stability in the modern infrastructure over a large area of the country. Loss of connectivity between the government and its populace would only exacerbate the consequences of such a scenario.

This analysis is based largely on selected case studies, including major blackouts, natural disasters, and terrorist incidents in recent U.S. history. These incidents served as approximate analogs in order to best predict the sociological and psychological effects of an EMP attack.

### Impact of an EMP Attack

While no single event serves as a model for an EMP scenario with incidence of long-lasting widespread power outage, communications failure, and other effects, the combined analysis of the following case studies provides useful insight in determining human reactions following an EMP attack:

Blackouts:

- ◆ Northeast (1965)
- ◆ New York (1977)

---

<sup>1</sup> Patrick, Eugene L., and William L. Vault, *Bioelectromagnetic Effects of the Electromagnetic Pulse (EMP)*, Adelphi, MD: Harry Diamond Laboratories, March 1990, pp. 6–7.

<sup>2</sup> Ibid, pp. 8–10.

<sup>3</sup> EMP Commission Staff Paper, Quick Look Pacemaker Assessment, December 2003.

<sup>4</sup> Sandia National Laboratory, EMP Commission-sponsored test.

- ◆ Hydro Quebec (1989)
- ◆ Western states (1996)
- ◆ Auckland, New Zealand (1998)
- ◆ Northeast (2003)

Natural Disasters:

- ◆ Hurricane Hugo (1989)
- ◆ Hurricane Andrew (1992)
- ◆ Midwest floods (1993)

Terrorist Incidents:

- ◆ World Trade Center attack (2001)
- ◆ Anthrax attacks (2001)

### **Blackouts**

In 1965, a blackout occurred over the northeastern United States and parts of Canada. New Hampshire; Vermont; Massachusetts; Connecticut; Rhode Island; New York, including metropolitan New York City; and a small part of Pennsylvania were in the dark after operators at Consolidated Edison were forced to shut down its generators to avoid damage. Street traffic was chaotic, and some people were trapped in elevators, but there were few instances of antisocial behavior while the lights were out.<sup>5</sup> It was a “long night in the dark,” but the recovery proceeded without incident, and citizens experienced relative civility.

*TIME* Magazine described New York’s next blackout, in 1977, as a “Night of Terror.”<sup>6</sup> Widespread chaos reigned in the city until power was restored — entire blocks were looted and set ablaze, people flipped over cars and vans on the streets; the city was in pandemonium. That night 3,776 arrests were made, and certainly not all looters, thieves, and arsonists were apprehended or arrested.<sup>7</sup> While this is a dramatic example of antisocial behavior following a blackout, sociologists point to extraordinary demographic and historical issues that contributed to the looting. For instance, extreme poverty and socio-economic inequality plagued New York neighborhoods, and many of the looters originated from the poorer sections of the city, engaging in “vigilante redistribution” by looting consumer goods and luxuries. Racial tensions were high, and a serial killer known as Son of Sam had recently terrorized New Yorkers.

In 1989, more than 6 million customers lost power when the geomagnetic storm discussed in Chapter 4 caused a massive power failure in Quebec. The electricity failures caused by this geomagnetic storm reached a much larger area than is typically affected by traditional blackouts resulting from technological failure. However, the outage lasted just over 9 hours, most of which were during the day.<sup>8</sup> The local and national papers were curiously silent about the blackout, and little to no unusual or adverse human behavior was attributed to the power loss. The event was most significantly a lesson for operators of the North American electric grids because it revealed vulnerabilities in the system.

---

<sup>5</sup> “The Great Northeast Blackout of 1965,” <http://www.ceet.niu.edu/faculty/vanmeer/outage.htm>.

<sup>6</sup> Sigwart, Charles P., “Night of Terror,” *Time*, July 25, 1977.

<sup>7</sup> “1977 New York Blackout,” Blackout History Project, <http://blackout.gmu.edu/events/tl1977.html>.

<sup>8</sup> Kappenman, John G., “Geomagnetic Storms Can Threaten Electric Power Grid,” *Earth in Space*, Vol. 9, No. 7, March 1997, pp.9-11. © 1997 American Geophysical Union. [http://www.agu.org/sci\\_soc/eiskappenman.html](http://www.agu.org/sci_soc/eiskappenman.html).

In 1998, Auckland, New Zealand, experienced a significant blackout that lasted more than 5 weeks and affected more than 1 million people.<sup>9</sup> Civility reigned for the duration of the outage, which was likely attributed to a number of factors, including:

- ◆ There was no significant threat to public health, because water and sewage infrastructures were functioning.
- ◆ In anticipation of potential incidents, police increased their presence in urban areas.
- ◆ The recovery process was underway nearly immediately, communicating to the public that the situation would eventually be under control.
- ◆ Nearly all blackout recovery resources of New Zealand were rushed to the capital for recovery efforts.

Recovery efforts from elsewhere in New Zealand were significant symbolically as well as practically, as demonstrated by the fact that electricity was available elsewhere. Businesses attempted to carry on as normally as possible, with some examples of opportunism, such as businesses relocating to more desirable spaces that had been vacated. Social consequences included criticism and blame of the authorities, both municipal and national, because the technological failures were attributed in large part to privatization of the power sector. However, this response never materialized into violence, crime, or social disorder.

Most recently, New York City and the eight states in the northeast experienced another significant blackout in August 2003. While the blackout inconvenienced many on a hot summer day, general civility remained intact. News coverage indicated that those affected by the blackout dealt with the obstacles quietly and even developed a sort of camaraderie while struggling through nights without running water and electricity. In contrast to the 1977 blackout, police made only 850 arrests the night of the 2003 blackout, of which “only 250 to 300 were directly attributable to the blackout,” indicating a slight decline from the average number of arrests on a given summer day.<sup>10</sup> While this blackout was widespread, it was not long lasting, and it did not interrupt the communications infrastructure significantly.

Blackouts provide only a partial picture of life following an EMP attack. Most blackouts are localized and are resolved quickly. Further, usually communication systems are not completely shut down, and major infrastructures can remain intact if significant portions of infrastructure hardware are located outside of the affected area. In order to best approximate the effects of longer-lasting, widespread infrastructure disruption—with or without electrical power failure—it is necessary to look to natural disasters for examples of human reaction.

### **Natural Disasters**

At the time that Hurricane Hugo hit in 1989, it was the most intense hurricane to strike Georgia and the Carolinas in 100 years. Surveys of Hurricane Hugo’s survivors indicate that some individuals who suffered personal and financial losses from the hurricane showed clinically significant symptoms of psychological trauma. According to some researchers, many of the adverse mental health effects of Hugo could be explained by deterioration in perceived social support. While on the whole, the rate of post-traumatic

<sup>9</sup> “Power failure brings New Zealand’s largest city to standstill,” CNN, <http://www.cnn.com/WORLD/9802/24/nzealand.blackout/index.html>.

<sup>10</sup> Adler, Jerry, et al, “The Day the Lights Went Out,” *Newsweek*; August 25, 2003, Vol. 142, Issue 8, p. 44.



stress disorder symptoms was low, stress effects lingered long after the hurricane's physical damage was repaired.

Hurricane Andrew blew through the southeastern United States and along the coast of the Gulf of Mexico in 1992, causing \$26.5 billion in damage. Andrew left 250,000 families homeless and 1.4 million families without electricity immediately following the hurricane. After such extraordinary destruction and disruption, it is perhaps not surprising that one-third of a sample of individuals met criteria for post-traumatic stress disorder 4 months after the hurricane.<sup>11</sup>

Hurricanes Hugo and Andrew demonstrated to psychologists that disaster-related declines in perceived support explained the difference in symptoms between the two disasters; deterioration was more significant in Andrew and recovery was weaker. In the long-lasting recovery period, Floridians saw looting, opportunism, and vigilante civil defense. Press coverage of Hurricane Andrew suggests that after a multi-state disaster, people will expect help, and they will expect it from the federal government, as well as from state and local authorities.

Flooding in the American Midwest in 1993 resulted in 25 deaths, affected more than 8 million acres, and cost billions of dollars in property damage and more than 2 billion dollars in crop damage. Water depths ranged from 11 feet of flooding in Minneapolis to 43 feet in St. Louis. Electricity was restored where possible within 3 days and in downtown Des Moines within 23 hours. The floods devastated families, businesses, and individuals, who lost nearly everything and were unable to control events throughout the recovery process. Thousands of people assisted in volunteer recovery efforts by sandbagging and providing needed supplies.<sup>12</sup> Most came from unaffected areas to help the most urgent victims. The floods provide an example of widespread damage crippling several infrastructures for a significant period of time and an example of a disaster in which regional experience may matter tremendously in disaster recovery.

Blackouts and natural disasters have limits as approximations of recovery following an EMP attack. An important element is the relevance of fear and individual panic in these situations versus what might occur following an EMP attack. For this component, it is useful to examine recent terrorist incidents in the United States in order to gauge the effects of fear among the public. Because terrorist attacks appear to be indiscriminate and random, they can arouse acute anxiety and feelings of helplessness, which shatter beliefs of invulnerability and even a belief in justice and order in the world.

### **Terrorist Incidents**

The attacks on the World Trade Center in New York on September 11, 2001, certainly qualified as seemingly indiscriminate and random. Following this disaster, in which nearly 3,000 people died, those in the immediate and surrounding area showed considerable psychological trauma and damage. Some individuals who experienced these attacks may have lost confidence in their abilities to cope and control outcomes. Overall, however, the survivors of the attacks proved remarkably resilient, flexible, and competent in the face of an arbitrary, violent, and completely unexpected attack.<sup>13</sup>

---

<sup>11</sup> Norris, et al, "60,000 Disaster Victims Speak: Part 1. An Empirical Review of the Empirical Literature, 1981-2001," *Psychiatry*, Fall 2002, 65, 3, Health Module.

<sup>12</sup> Barnes, Harper, "The Flood of 1993," *St. Louis Post-Dispatch*, July 25, 1993.

<sup>13</sup> Kendra, James, and Tricia Wachtendorf, "Elements of Resilience in the World Trade Center Attack," Disaster Research Center, 2001.

In October 2001, a month following the attack on the World Trade Center, Americans saw a series of anthrax-infected mail pieces threatening intended mail recipients and handlers. The death toll was small (five individuals), but public concern was considerable. This period is an example of public response to an adversary-initiated threat that disrupted infrastructure. The public demonstrated a great need for control over the situation, through preparedness and information. For example, many Americans took protective measures, despite the astronomical odds against infection. The news media were saturated with reports of anthrax infections, suspected infections, and general information about anthrax and how to respond to infection. Though no culprit was apprehended, the attacks stopped, and normal postal activity resumed.

### ***Some Lessons Learned***

Though the United States has not experienced a severe, widespread disruption to infrastructure comparable to an EMP attack, the cases reviewed provide some practical direction for predictions of behavior. For example, it can be expected that emotional reactions such as shock and paralysis that have followed past disasters could be magnified in a large-scale event such as an EMP attack. In particular, the paralysis of government assistance entities, such as law enforcement and emergency services, would aggravate this effect. In most instances, social disorder would be minimal, in significant part, due to the knowledge that authorities are in control of the situation. Without that assurance from an outside source, it appears likely that people would turn to immediate neighbors or community members for information and support, if possible.

Following disruptive disasters, information is among the most pressing needs for individuals. Not surprisingly, people's first concerns are the whereabouts and safety of their family members and friends. Another urgent priority is an understanding of the situation — knowledge of what has happened, who and what is affected, and the cause of the situation. A related yet distinct information need is for confirmation that the situation will be resolved, either from common sense and experience, in the case of a small-scale disaster, or from the involvement of local or federal authorities, in the case of a large-scale disaster. Psychologists note that dramatic events force people to reexamine their basic understanding about the world, and that survivors need to process an event before they can fully absorb it. This information processing begins the alternating phases of intrusion and avoidance that are primary indicators of post-traumatic stress.<sup>14</sup>

The aftermath of natural disasters is often marked by instances or a period of considerable pro-social behavior such as cooperation, social solidarity, and acts of selflessness. However, this encouraging observation might not be similarly magnified in projections for human behavior following an EMP attack. The key intangible, immeasurable difference is the knowledge that normal order would resume, based on significant indicators.

It is important to note some of the differences between natural disasters and technological disasters, particularly those caused by human intent. Natural disasters “create a social context marked by an initial overwhelming consensus regarding priorities and the allocation of resources,”<sup>15</sup> which explains the enormous outpouring of voluntary support following the floods of 1993. In contrast to natural disasters, which “occur as purpose-

---

<sup>14</sup> Norris, et al, “60,000 Disaster Victims Speak: Part II. Summary and Implications of the Disaster Mental Health Research,” *Psychiatry*, Fall 2002, 65, 3, Health Module.

<sup>15</sup> Warheit, G.J., “A note on natural disasters and civil disturbances: Similarities and differences.” *Mass Emergencies*, 1, 1976, pp. 131-137.

less, asocial events; civil disturbances can be viewed as instrumentally initiated to achieve certain social goals.”<sup>16</sup> An EMP attack would certainly be perceived similarly, whether the adversary were a terrorist organization or a state.

The selected case studies provide only an approximation of EMP effects. For example, the effects of the knowledge that widespread infrastructure disruption resulted from an intentional foreign attack are yet unknown. Much evidence points to people’s resilience in the immediate aftermath of disasters. However, during a lengthy recovery process, as would be expected following an EMP attack with widespread, long-duration effects, the psychological effects of the attack should not be underestimated.

It appears clear that the most crucial question in the task of avoiding social disorder is how to establish communication without electricity immediately following an EMP attack. Without communication alternatives, it would be impossible to alert people to the availability of emergency supplies or inform them concerning emergency response activities. It also appears clear that greater awareness of the nature of an EMP attack and knowledge of what prudent preparations might be undertaken to mitigate its consequences would be desirable. Accordingly we make the following recommendations.

### Recommendations

- ◆ Support to national leadership should involve measures to ensure that the President can communicate effectively with the citizenry.
- ◆ Because many citizens would be without power, communications, and other services for days — or perhaps substantially longer — before full recovery could occur, during that interval, it will be crucial to provide a reliable channel of information to citizens to let them know what has happened, what the current situation is, when help of what types might be available, what their governments are doing, and answers to the host of other questions that, if not answered, would almost certainly create more instability and suffering for the affected individuals, communities, and the Nation as a whole. In particular:
  - The Department of Homeland Security should play a leading role in spreading knowledge of the nature of prudent mitigation preparations for EMP attack to mitigate its consequences.
  - The Department of Homeland Security should add content to Web sites it maintains, such as [www.Ready.gov](http://www.Ready.gov), which provides concise overviews of the threats posed by EMP attacks and geomagnetic storms, summarizes steps that people should take given an incident and identifies alternate or emergency communications channels.
  - The Department of Homeland Security should work with state homeland security organizations to develop and exercise communications networks involving the organizations that normally operate in each community.

---

<sup>16</sup> Ibid.

## Appendix A. The Commission and Its Charter

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack was established by Congress through Title XIV of Public Law 106-398. Looking out 15 years, the Commission was tasked to assess:

- 1) The nature and magnitude of potential high-altitude EMP threats to the United States from all potentially hostile states or non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to perform a high-altitude EMP attack against the United States within the next 15 years.
- 2) The vulnerability of United States military and especially civilian systems to an EMP attack, giving special attention to vulnerability of the civilian infrastructure as a matter of emergency preparedness.
- 3) The capability of the United States to repair and recover from damage inflicted on United States military and civilian systems by an EMP attack.
- 4) The feasibility and cost of hardening select military and civilian systems against EMP attack.

The Commission was also tasked to recommend any steps it believes should be taken by the United States to better protect its military and civilian systems from EMP attack.

In accord with its charter, the Commission focused on the electromagnetic pulse produced by high-altitude nuclear weapon detonations, as opposed to other types of nuclear and non-nuclear EMP phenomena. Unless clearly indicated to the contrary, all references to EMP are to the electromagnetic pulse produced by a high-altitude nuclear detonation.

This report presents the unanimous conclusions and recommendations of the Commissioners.

### Organization

Commissioners were nominated by the Secretary of Defense and by the Administrator of the Federal Emergency Management Agency<sup>1</sup>:

- ◆ Dr. William R. Graham (Chairman)
- ◆ Dr. John S. Foster, Jr.
- ◆ Mr. Earl Gjelde
- ◆ Dr. Robert J. Hermann
- ◆ Mr. Henry (Hank) M. Kluepfel
- ◆ Gen Richard L. Lawson, USAF (Ret.)
- ◆ Dr. Gordon K. Soper
- ◆ Dr. Lowell J. Wood, Jr.
- ◆ Dr. Joan B. Woodard

Commissioners brought to this task a wide range of expertise, including service as an advisor to the President; senior management experience in both civilian and military agencies, National Laboratories, and the corporate sector; management and operation of national infrastructures, and technical expertise in the design of nuclear weapons and in the hardening of systems against nuclear weapon effects. Commissioner resumes are provided in an appendix to this volume.

---

<sup>1</sup> The Federal Emergency Management Agency was an independent agency when the Commission was established; it is now a component within the Department of Homeland Security.

Dr. Michael J. Frankel served as Executive Director of the Commission. He was also responsible for overseeing the technical efforts in support of the Commission accomplished by both American and foreign organizations. The Institute for Defense Analysis, under the leadership of Dr. Rob Mahoney, provided staff and facilities support for the Commission. Dr. Peter Pry provided liaison with the Congress. The Commission also benefited from the understanding of EMP available in foreign institutions. Several government, non-profit, and commercial organizations conducted work and prepared reports for the Commission.

## Method

The Commission employed a capabilities-based methodology to assess potential high-altitude EMP threats to the United States over the next 15 years.<sup>2</sup> To this end it engaged the current Intelligence Community, sponsored the acquisition of new test data and performed analytic studies as input to the independent assessment developed by the Commission. Fifteen years is a very long time horizon. Many developments are possible, to include actions by the United States and others that can shape this future in a variety of ways. At the Commission's inception, Iraq was a state of concern from the standpoint of nuclear proliferation and potential EMP threats. Due to actions taken by the Coalition, such Iraqi capabilities are no longer a current concern.

...a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered looks strange; what looks strange is therefore improbable; what seems improbable need not be considered seriously.

— Thomas C. Schelling, in Roberta Wohlstetter, *Pearl Harbor: Warning and Decision*. Stanford University Press, 1962, p. vii

The Commission did not attempt to forecast the relative likelihood of alternative WMD threat scenarios. Instead, it sponsored research and reviewed existing assessments to identify the capabilities that might be available to adversaries, with particular emphasis on ballistic missile and nuclear weapons needed for EMP attacks.

The Commission's charter encompassed all types of high-altitude EMP threats. The Commission made a decision to focus most of its efforts on the most feasible of these threats – EMP attacks involving one or a few weapons that could cause serious damage to the functioning of the United States as a society or result in undermining national support to American forces during a regional contingency.

## Activities

The Commission received excellent support from the Intelligence Community, particularly the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, and Department of Energy Office of Intelligence. National Nuclear Security Administration laboratories (Lawrence Livermore, Los Alamos, and Sandia), the Navy, and the Defense Threat Reduction Agency provided excellent technical support to the Commission's analyses. While it benefited from these inputs, the Commission developed an independent assessment, and is solely responsible for the content of its research, conclusions, and recommendations in this report.

<sup>2</sup> This methodology is addressed in a Commission staff paper — Rob Mahoney, *Capabilities-Based Methodology for Assessing Potential Adversary Capabilities*, March 2004.

The Commission also reviewed relevant foreign research and programs, and assessed foreign perspectives on EMP attacks.

In considering EMP, the Commission also gave attention to the coincident nuclear effects that would result from a high-altitude detonation that produces EMP, e.g., possible disruption of the operations of, or damage to, satellites in a range of orbits around the Earth.

In addition to examining potential threats, the Commission was charged to assess U.S. vulnerabilities (civilian and military) to EMP and to recommend measures to counter EMP threats. For these purposes, the Commission reviewed research and best practices within the United States and other countries.

Early in this review it became apparent that only limited EMP vulnerability testing had been accomplished for modern electronic systems and components. To partially remedy this deficit, the Commission sponsored illustrative testing of current systems and infrastructure components.





## Appendix B. Biographies

*Dr. William R. Graham* is Chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. He is the retired Chairman of the Board and Chief Executive Officer of National Security Research Inc. (NSR), a Washington-based company that conducted technical, operational, and policy research and analysis related to U.S. national security. He currently serves as a member of the Department of Defense's Defense Science Board and the National Academies Board on Army Science and Technology. In the recent past he has served as a member of several high-level study groups, including the Department of Defense Transformation Study Group, the Commission to Assess United States National Security Space Management and Organization, and the Commission to Assess the Ballistic Missile Threat to the United States. From 1986–89 Dr. Graham was the director of the White House Office of Science and Technology Policy, while serving concurrently as Science Advisor to President Reagan, Chairman of the Federal Joint Telecommunications Resources Board, and a member of the President's Arms Control Experts Group.

*Dr. John S. Foster, Jr.*, is Chairman of the Board of GKN Aerospace Transparency Systems, and consultant to Northrop Grumman Corporation, Technology Strategies & Alliances, Sikorsky Aircraft Corp., Intellectual Ventures, Lawrence Livermore National Lab, Ninesigma, and Defense Group. He retired from TRW as Vice President, Science and Technology, in 1988 and continued to serve on the Board of Directors of TRW from 1988 to 1994. Dr. Foster was Director of Defense Research and Engineering for the Department of Defense from 1965–1973, serving under both Democratic and Republican administrations. In other distinguished service, Dr. Foster has been on the Air Force Scientific Advisory Board, the Army Scientific Advisory Panel, and the Ballistic Missile Defense Advisory Committee, Advanced Research Projects Agency. Until 1965, he was a panel consultant to the President's Science Advisory Committee, and from 1973–1990 he was a member of the President's Foreign Intelligence Advisory Board. He is a member of the Defense Science Board, which he chaired from January 1990–June 1993. From 1952–1962, Dr. Foster was with Lawrence Livermore National Laboratory (LLNL), where he began as a Division Leader in experimental physics, became Associate Director in 1958, and became Director of LLNL and Associate Director of the Lawrence Berkeley National Laboratory in 1961.

*Mr. Earl Gjelde* is the President and Chief Executive Officer of Summit Power Group Inc., and several affiliated companies, primary participants in the development of over 5,000 megawatts of natural gas fired electric and wind generating plants within the United States. He has served on the boards of EPRI and the U.S. Energy Association among others. He has held a number of U.S.A. government posts, serving as President George Herbert Walker Bush's Under (now called Deputy) Secretary and Chief Operating Officer of the U.S. Department of the Interior (1989) and serving President Ronald Reagan as Under Secretary and Chief Operating Officer of the U.S. Department of the Interior (1985–1988), the Counselor to the Secretary and Chief Operating Officer of the U.S. Department of Energy (1982–1985); and Deputy Administrator, Power Manager and Chief Operating Officer of the Bonneville Power Administration (1980–1982). While in the Reagan Administration he served concurrently as Special Envoy to China (1987), Deputy Chief of Mission for the U.S.-Japan Science and Technology Treaty (1987–1988), and Counselor for Policy to the Director of the National Critical Materials Council

(1986–1988). Prior to 1980, he was a Principal Officer of the Bonneville Power Administration.

*Dr. Robert J. Hermann* is a Senior Partner of Global Technology Partners, LLC, a consulting firm that focuses on technology, defense aerospace, and related businesses worldwide. In 1998, Dr. Hermann retired from United Technologies Corporation (UTC), where he was Senior Vice President, Science and Technology. Prior to joining UTC in 1982, Dr. Hermann served 20 years with the National Security Agency with assignments in research and development, operations, and NATO. In 1977, he was appointed Principal Deputy Assistant Secretary of Defense for Communications, Command, Control, and Intelligence. In 1979, he was named Assistant Secretary of the Air Force for Research, Development, and Logistics and concurrently was Director of the National Reconnaissance Office.

*Mr. Henry (Hank) M. Kluepfel* is a Vice President for Corporate Development at SAIC. He is the company's leading cyberspace security advisor to the President's National Security Telecommunications Advisory Committee (NSTAC) and the Network Reliability and Interoperability Council (NRIC). Mr. Kluepfel is widely recognized for his 30-plus years of experience in security technology research, design, tools, forensics, risk reduction, education, and awareness, and he is the author of industry's de facto standard security base guideline for the Signaling System Number 7(SS7) networks connecting and controlling the world's public telecommunications networks. In past affiliations with Telcordia Technologies (formerly Bellcore), AT&T, BellSouth and Bell Labs, he led industry efforts to protect, detect, contain, and mitigate electronic and physical intrusions and led the industry's understanding of the need to balance technical, legal, and policy-based countermeasures to the then emerging hacker threat. He is recognized as a Certified Protection Professional by the American Society of Industrial Security and is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

*General Richard L. Lawson, USAF (Ret.)*, is Chairman of Energy, Environment and Security Group, Ltd., and former President and CEO of the National Mining Association. He also serves as Vice Chairman of the Atlantic Council of the U.S.; Chairman of the Energy Policy Committee of the U.S. Energy Association; Chairman of the United States delegation to the World Mining Congress; and Chairman of the International Committee for Coal Research. Active duty positions included serving as Military Assistant to the President; Commander, 8th Air Force; Chief of Staff, Supreme Headquarters Allied Powers Europe; Director for Plans and Policy, Joint Chiefs of Staff; Deputy Director of Operations, Headquarters U.S. Air Force; and Deputy Commander in Chief, U.S. European Command.

*Dr. Gordon K. Soper* is employed by Defense Group Inc. There he has held various senior positions where he was responsible for broad direction of corporate goals relating to company support of government customers in areas of countering the proliferation of weapons of mass destruction, nuclear weapons effects and development of new business areas and growth of technical staff. He provides senior-level technical support on a range of task areas to the Defense Threat Reduction Agency (DTRA) and to a series of Special Programs for the Office of the Secretary of Defense and the White House Military Office. Previously, Dr. Soper was Principal Deputy to the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Programs (ATSD(NCB)); Director, Office of Strategic and Theater Nuclear Forces Command, Control and Communications (C3) of

the Office of the Assistant Secretary of Defense (C3I); Associate Director for Engineering and Technology/Chief Scientist at the Defense Communications Agency (now DISA); and held various leadership positions at the Defense Nuclear Agency (now DTRA).

*Dr. Lowell L. Wood, Jr.*, is a scientist-technologist who has contributed to technical aspects of national defense, especially defense against missile attack, as well as to controlled thermonuclear fusion, laser science and applications, optical and underwater communications, very high-performance computing and digital computer-based physical modeling, ultra-high-power electromagnetic systems, space exploration and climate-stabilization geophysics. Wood obtained his Ph.D. in astrophysics and planetary and space physics at UCLA in 1965, following receipt of bachelor's degrees in chemistry and math in 1962. He has held faculty and professional research staff appointments at the University of California (from which he retired after more than four decades in 2006) and is a Research Fellow at the Hoover Institution at Stanford University. He has advised the U.S. Government in many capacities, and has received a number of awards and honors from both government and professional bodies. Wood is the author, co-author or editor of more than 200 unclassified technical papers and books and more than 300 classified publications, and is named as an inventor on more than 200 patents and patents-pending.

*Dr. Joan B. Woodard* is Executive Vice President and Deputy Laboratories Director for Nuclear Weapons at Sandia National Laboratories. Sandia's role is to provide engineering support and design to the Nation's nuclear weapons stockpile, provide our customers with research, development, and testing services, and manufacture specialized non-nuclear products and components for national defense and security applications. The laboratories enable safe and secure deterrence through science, engineering, and management excellence. Prior to her current assignment, Dr. Woodard served as Executive Vice President and Deputy Director, responsible for Sandia's programs, operations, staff and facilities; developing policy and assuring implementation; and strategic planning. Her Sandia history began in 1974, and she rose through the ranks to become the Director of the Environmental Programs Center and the Director of the Product Realization Weapon Components Center; Vice President of the Energy & Environment Division and Vice President of the Energy Information and Infrastructure Technologies Division. Joan has been elected to the Phi Kappa Phi Honor Society and has served on numerous external panels and boards, including the Air Force Scientific Advisory Board, the National Academy of Sciences' Study on Science and Technology for Countering Terrorism, the Secretary of Energy's Nuclear Energy Research Advisory Council, the Congressional Commission on Electromagnetic Pulse, and the Intelligence Science Board. Joan has received many honors, including the Upward Mobility Award from the Society of Women Engineers, and was named as "One of Twenty Women to Watch in the New Millennium" by the Albuquerque Journal. She also received the Spirit of Achievement Award from National Jewish Hospital.

*Dr. Michael J. Frankel* is Executive Director of the EMP Commission and one of the Nation's leading experts on the effects of nuclear weapons. Formerly he served as Associate Director for Advanced Energetics and Nuclear Weapons, Office of the Deputy Undersecretary of Defense (S&T); Chief Scientist, Nuclear Phenomenology Division, Defense Threat Reduction Agency; Congressional Fellow, U.S. Senate; Chief Scientist, Strategic Defense Initiative Organization Lethality Program; and as a Research Physicist at the Naval Surface Warfare Center, White Oak. In prior government service, Dr.

Frankel directed significant elements of the core national Nuclear Weapons Phenomenology program along with major WMD, Directed Energy, and Space System technology programs at the Defense Nuclear Agency while coordinating activities between the Military Services, National Laboratories, and industrial S&T organizations to address strategic defense technology needs. He has been an active participant in international scientific exchanges in his role as Executive Secretary for the U.S. – United Kingdom Joint Working Group under terms of the 1958 Atomic Treaty, and as Chairman of both the Novel Energetics and Hard Target Defeat working groups under the TTCP agreement with the UK, Australia, Canada and New Zealand. He has also delivered invited lectures, chaired national and international technical symposia, and published numerous articles in the professional scientific literature. He holds a Ph.D. in Theoretical Physics from New York University.





ISBN 978-0-16-080927-9



9 780160 809279

# Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

## *Volume 1: Executive Report* *2004*

Dr. John S. Foster, Jr.

Mr. Earl Gjelde

Dr. William R. Graham (Chairman)

Dr. Robert J. Hermann

Mr. Henry (Hank) M. Kluepfel

GEN Richard L. Lawson, USAF (Ret.)

Dr. Gordon K. Soper

Dr. Lowell L. Wood, Jr.

Dr. Joan B. Woodard



## CHARTER

Public Law 106-398, Title XIV

### SEC. 1402. DUTIES OF COMMISSION

(a) Review of EMP Threat. The Commission shall assess:

(1) the nature and magnitude of potential high-altitude EMP threats to the United States from all potentially hostile states or non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to perform a high-altitude EMP attack against the United States within the next 15 years;

(2) the vulnerability of United States military and especially civilian systems to an EMP attack, giving special attention to vulnerability of the civilian infrastructure as a matter of emergency preparedness;

(3) the capability of the United States to repair and recover from damage inflicted on United States military and civilian systems by an EMP attack; and

(4) the feasibility and cost of hardening select military and civilian systems against EMP attack.

(b) Recommendation. The Commission shall recommend any steps it believes should be taken by the United States to better protect its military and civilian systems from EMP attack.

The findings and recommendations presented in this report are the independent judgments of this Commission and should not be attributed to any other people or organizations. This report presents the unanimous views of the Commissioners.



## ABSTRACT

Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse (EMP). A determined adversary can achieve an EMP attack capability without having a high level of sophistication.

EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences. EMP will cover the wide geographic region within line of sight to the nuclear weapon. It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of US society, as well as to the ability of the United States and Western nations to project influence and military power.

The common element that can produce such an impact from EMP is primarily electronics, so pervasive in all aspects of our society and military, coupled through critical infrastructures. Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow. The impact of EMP is asymmetric in relation to potential protagonists who are not as dependent on modern electronics.

The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected. Correction is feasible and well within the Nation's means and resources to accomplish.





# CONTENTS

OVERVIEW: EMP IS CAPABLE OF CAUSING CATASTROPHE FOR THE NATION.....	1
WE CAN PREVENT AN EMP CATASTROPHE.....	4
Nature of the EMP Threat.....	4
Prevention .....	7
Protection and Recovery of Civilian Infrastructures .....	8
STRATEGY AND RECOMMENDATIONS .....	11
Intelligence, Interdiction, and Deterrence.....	11
Protecting Critical Components of the Infrastructure.....	12
Maintaining the Capability to Monitor and Evaluate the Condition of Critical Infrastructures.....	12
Recognizing EMP Attack .....	12
Planning to Carry Out a Systematic Recovery of Critical Infrastructures.....	14
Training, Evaluating, Red Teaming, and Periodically Reporting to the Congress.....	14
Defining the Federal Government’s Responsibility and Authority to Act .....	15
Recognizing the Opportunities for Shared Benefits .....	16
Conducting Research and Development.....	16
ELECTRIC POWER INFRASTRUCTURE .....	17
Nature of the Problem.....	17
Recommended Mitigation and Responsibility.....	19
Protection .....	20
Restoration .....	20
Essential Component Protection .....	21
System Restoration .....	22
TELECOMMUNICATIONS .....	24
Importance of Assured Telecommunications .....	24
EMP Effects on Telecommunications .....	28
Recommended Mitigation Activities .....	28

BANKING AND FINANCE.....	31
Nature of the Problem.....	31
Recommended Mitigation and Responsibility.....	33
FUEL/ENERGY INFRASTRUCTURE.....	35
TRANSPORTATION INFRASTRUCTURE.....	36
Nature of the Problem.....	36
Strategy for Protection and Recovery.....	37
FOOD INFRASTRUCTURE .....	40
Nature of the Problem.....	40
Mitigation and Responsibility.....	40
WATER SUPPLY INFRASTRUCTURE .....	42
EMERGENCY SERVICES .....	43
Vulnerabilities.....	43
Recommended Strategy for Protection and Recovery.....	43
SPACE SYSTEMS.....	44
GOVERNMENT.....	45
KEEPING THE CITIZENRY INFORMED.....	46
PROTECTION OF MILITARY FORCES .....	47

## APPENDIXES

A The Commission and Its Method.....	A-1
B Commissioners.....	B-1

## FIGURES

1 Starfish Nuclear Detonation.....	5
2 Illustrative EMP Effects – Fast Pulse .....	6
3 Illustrative EMP Effects – Slow Pulse Protection and Recovery of Civilian Infrastructures .....	7
4 Interdependent Infrastructure Sectors.....	9
5 Extent of 1989 Geomagnetic Storm.....	17

## OVERVIEW

### EMP IS CAPABLE OF CAUSING CATASTROPHE FOR THE NATION

The high-altitude nuclear weapon-generated electromagnetic pulse (EMP) is one of a small number of threats that has the potential to hold our society seriously at risk and might result in defeat of our military forces.

Briefly, a single nuclear weapon exploded at high altitude above the United States will interact with the Earth's atmosphere, ionosphere, and magnetic field to produce an electromagnetic pulse (EMP) radiating down to the Earth and additionally create electrical currents in the Earth. EMP effects are both direct and indirect. The former are due to electromagnetic "shocking" of electronics and stressing of electrical systems, and the latter arise from the damage that "shocked"—upset, damaged, and destroyed—electronics controls then inflict on the systems in which they are embedded.

*The damage level could be sufficient to be catastrophic to the Nation, and our current vulnerability invites attack.*

The indirect effects can be even more severe than the direct effects.

The electromagnetic fields produced by weapons designed and deployed with the intent to produce EMP have a high likelihood of damaging electrical power systems, electronics, and information systems upon which American society depends. Their effects on dependent systems and infrastructures could be sufficient to qualify as catastrophic to the Nation.

Depending on the specific characteristics of the attacks, unprecedented cascading failures of our major infrastructures could result. In that event, a regional or national recovery would be long and difficult and would seriously degrade the safety and overall viability of our Nation. The primary avenues for catastrophic damage to the Nation are through our electric power infrastructure and thence into our telecommunications, energy, and other infrastructures. These, in turn, can seriously impact other important aspects of our Nation's life, including the financial system; means of getting food, water, and medical care to the citizenry; trade; and production of goods and services. The recovery of any one of the key national infrastructures is dependent on the recovery of others. The longer the outage, the more problematic and uncertain the recovery will be. It is possible

for the functional outages to become mutually reinforcing until at some point the degradation of infrastructure could have irreversible effects on the country's ability to support its population.

EMP effects from nuclear bursts are not new threats to our nation. The Soviet Union in the past and Russia and other nations today are potentially capable of creating these effects. Historically, this application of nuclear weaponry was mixed with a much larger population of nuclear devices that were the primary source of destruction, and thus EMP as a weapons effect was not the primary focus. Throughout the Cold War, the United States did not try to protect its civilian infrastructure against either the physical or EMP impact of nuclear weapons, and instead depended on deterrence for its safety.

What is different now is that some potential sources of EMP threats are difficult to deter—they can be terrorist groups that have no state identity, have only one or a few weapons, and are motivated to attack the US without regard for their own safety. Rogue states, such as North Korea and Iran, may also be developing the capability to pose an EMP threat to the United States, and may also be unpredictable and difficult to deter.

Certain types of relatively low-yield nuclear weapons can be employed to generate potentially catastrophic EMP effects over wide geographic areas, and designs for variants of such weapons may have been illicitly trafficked for a quarter-century.

China and Russia have considered limited nuclear attack options that, unlike their Cold War plans, employ EMP as the primary or sole means of attack. Indeed, as recently as May 1999, during the NATO bombing of the former Yugoslavia, high-ranking members of the Russian Duma, meeting with a US congressional delegation to discuss the Balkans conflict, raised the specter of a Russian EMP attack that would paralyze the United States.

Another key difference from the past is that the US has developed more than most other nations as a modern society heavily dependent on electronics, telecommunications, energy, information networks, and a rich set of financial and transportation systems that leverage modern technology. This asymmetry is a source of substantial economic, industrial, and societal advantages, but it creates vulnerabilities and critical interdependencies that are potentially disastrous to the United States. Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack. The current vulnerability of US

critical infrastructures can both invite and reward attack if not corrected; however, correction is feasible and well within the Nation's means and resources to accomplish.



## WE CAN PREVENT AN EMP CATASTROPHE

The Nation's vulnerability to EMP that gives rise to potentially large-scale, long-term consequences can be reasonably and readily reduced below the level of a potentially catastrophic national problem by coordinated and focused effort between the private and public sectors of our country. The cost for such improved security in the next 3 to 5 years is modest by any standard—and extremely so in relation to both the war on terror and the value of the national infrastructures involved. The appropriate response to this threatening situation is a balance of prevention, protection, planning, and preparations for recovery. Such actions are both rational and feasible. A number of these actions also reduce vulnerabilities to other serious threats to our infrastructures, thus giving multiple benefits.

### NATURE OF THE EMP THREAT

High-altitude EMP results from the detonation of a nuclear warhead at altitudes of about 40 to 400 kilometers above the Earth's surface. The immediate effects of EMP are disruption of, and damage to, electronic systems and electrical infrastructure. EMP is not reported in the scientific literature to have direct effects on people in the parameter range of present interest.

EMP and its effects were observed during the US and Soviet atmospheric test programs in 1962. Figure 1 depicts the Starfish nuclear detonation—not designed or intended as a generator of EMP—at an altitude of about 400 kilometers above Johnston Island in the Pacific Ocean. Some electronic and electrical systems in the Hawaiian Islands, 1400 kilometers distant, were affected, causing the failure of street-lighting systems, tripping of circuit breakers, triggering of burglar alarms, and damage to a telecommunications relay facility. In their testing that year, the Soviets executed a series of nuclear detonations in which they exploded 300 kiloton weapons at approximately 300, 150, and 60 kilometers above their test site in South Central Asia. They report that on each shot they observed damage to overhead and underground buried cables at distances of 600 kilometers. They also observed surge arrestor burnout, spark-gap breakdown, blown fuses, and power supply breakdowns.

What is significant about an EMP attack is that one or a few high-altitude nuclear detonations can produce EMP effects that can potentially disrupt or damage electronic

and electrical systems over much of the United States, virtually simultaneously, at a time determined by an adversary.



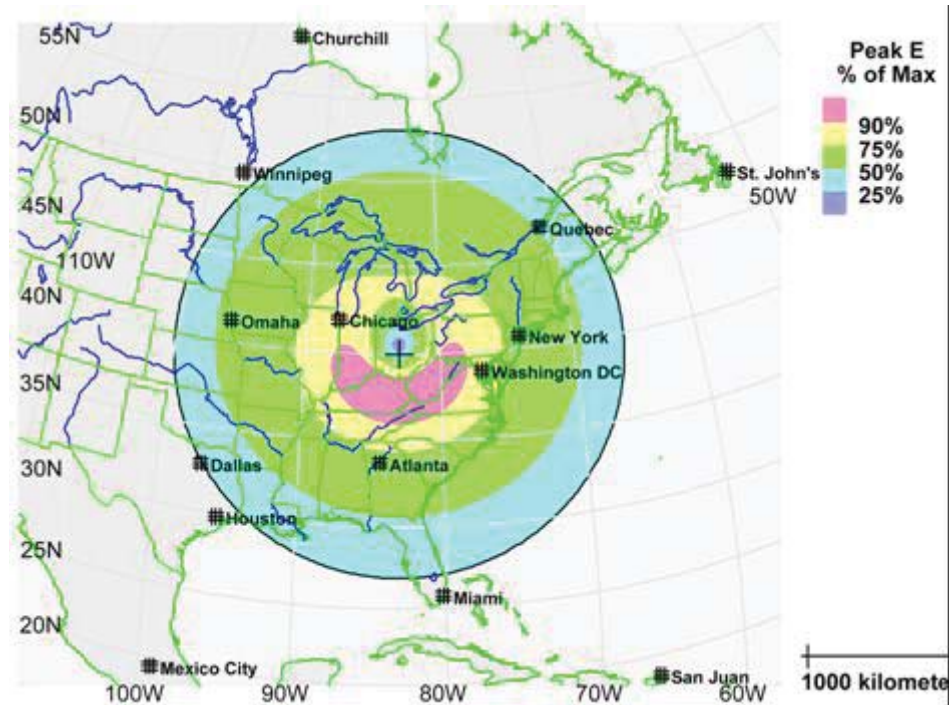
Widespread red air glow (6300 Å) amid dark clouds, caused mostly by x-ray-excited atomic oxygen (i.e., oxygen by photoelectrons liberated by Starfish X-rays)

### **Figure 1. Starfish Nuclear Detonation**

Gamma rays from a high-altitude nuclear detonation interact with the atmosphere to produce a radio-frequency wave of unique, spatially varying intensity that covers everything within line-of-sight of the explosion's center point. It is useful to focus on three major EMP components.

#### *FIRST EMP COMPONENT (E1)*

The first component is a free-field energy pulse with a rise-time measured in the range of a fraction of a billionth to a few billionths of a second. It is the "electromagnetic shock" that disrupts or damages electronics-based control systems, sensors, communication systems, protective systems, computers, and similar devices. Its damage or functional disruption occurs essentially simultaneously over a very large area, as illustrated in Figure 2.



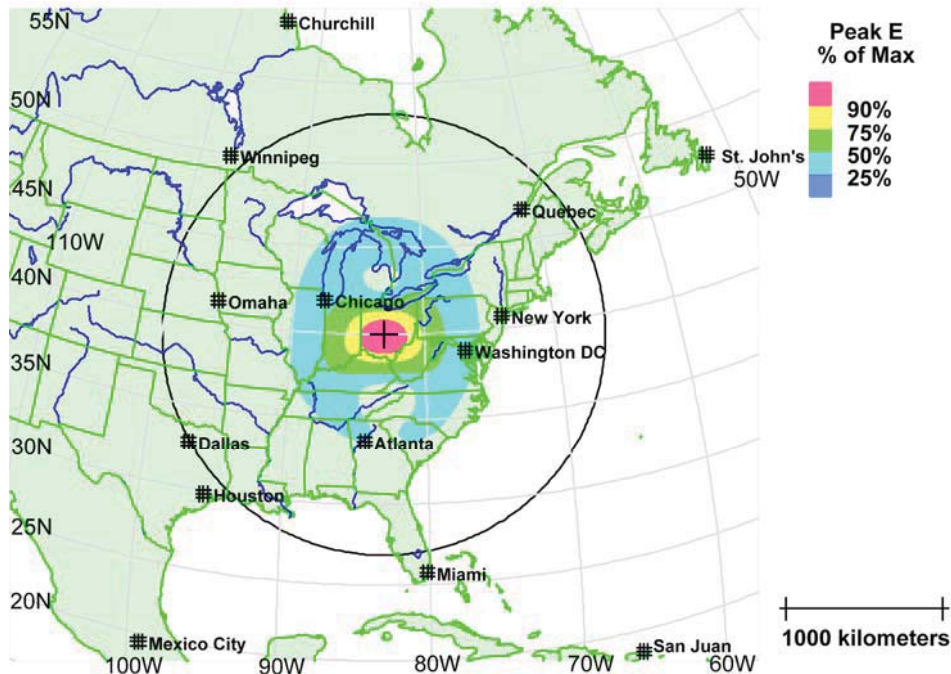
**Figure 2. Illustrative EMP Effects – Fast Pulse**

### *SECOND EMP COMPONENT (E2)*

The middle-time component covers roughly the same geographic area as the first component and is similar to lightning in its time-dependence, but is far more geographically widespread in its character and somewhat lower in amplitude. In general, it would not be an issue for critical infrastructure systems since they have existing protective measures for defense against occasional lightning strikes. The most significant risk is synergistic, because the E2 component follows a small fraction of a second after the first component's insult, which has the ability to impair or destroy many protective and control features. The energy associated with the second component thus may be allowed to pass into and damage systems.

### *THIRD EMP COMPONENT (E3)*

The final major component of EMP is a subsequent, slower-rising, longer-duration pulse that creates disruptive currents in long electricity transmission lines, resulting in damage to electrical supply and distribution systems connected to such lines (Figure 3). The sequence of E1, E2, and then E3 components of EMP is important because each can cause damage, and the later damage can be increased as a result of the earlier damage. In the example depicted in Figures 2 and 3, about 70% of the total electrical power load of the United States is within the region exposed to the EMP event.



**Figure 3. Illustrative EMP Effects – Slow Pulse Protection and Recovery of Civilian Infrastructures**

#### PREVENTION

An EMP attack is one way for a terrorist activity to use a small amount of nuclear weaponry—potentially just one weapon—in an effort to produce a catastrophic impact on our society, but it is not the only way. In addition, there are potential applications of surface-burst nuclear weaponry, biological and chemical warfare agents, and cyber attacks that might cause damage that could reach large-scale, long-term levels. The first order of business is to prevent any of these attacks from occurring.

The US must establish a global environment that will profoundly discourage such attacks. We must persuade nations to forgo obtaining nuclear weapons or to provide acceptable assurance that these weapons will neither threaten the vital interests of the United States nor fall into threatening hands.

For all others, we must make it difficult and dangerous to acquire the materials to make a nuclear weapon and the means to deliver them. We must hold at risk of capture or destruction anyone who has such weaponry, wherever they are in the world.

*The first order of business is to prevent any of these attacks from occurring.*

Those who engage in or support these activities must be made to understand that they do so at the risk of everything they value. Those who harbor or help those who conspire to create these weapons must suffer serious consequences as well.

In case these measures do not completely succeed, we must have vigorous interdiction and interception efforts to thwart delivery of all such weaponry. To support this strategy, the US must have intelligence capabilities sufficient to understand what is happening at each stage of developing threats. In summary, the costs of mounting such attacks must be made to be great in all respects, and the likelihood of successful attack rendered unattractively small.

The current national strategy for war on terrorism already contains all of these elements. The threat of an EMP attack further raises what may be at stake.

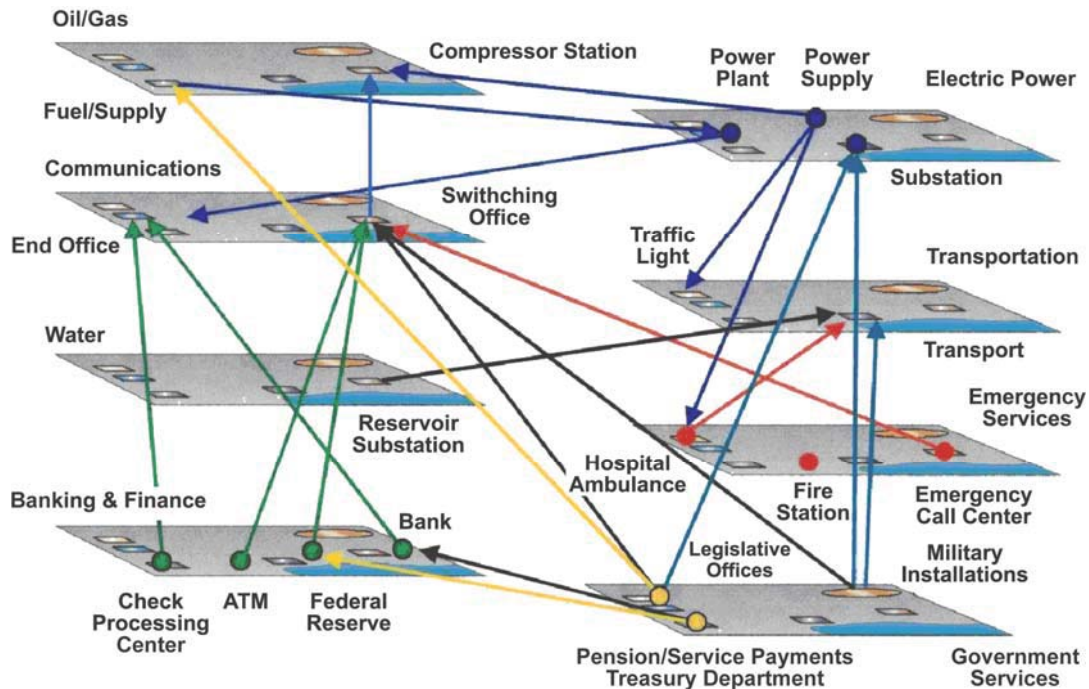
To further forestall an EMP attack, we must reduce our vulnerability to EMP and develop our ability to recover, should there be an attack, in order to reduce the incentives to use such weaponry. We should never allow terrorists or rogue states a “cheap shot” that has such a large and potentially devastating impact.

#### PROTECTION AND RECOVERY OF CIVILIAN INFRASTRUCTURES

Each critical infrastructure in the US is dependent upon other infrastructures (Figure 4). The interdependence on the proper functioning of such systems constitutes a hazard when threat of widespread failures exists. The strong interdependence of our critical national infrastructures may cause unprecedented challenges in attempts to recover from the widespread disruption and damage that would be caused by an EMP attack.

All of the critical functions of US society and related infrastructures—electric power, telecommunications, energy, financial, transportation, emergency services, water, food, etc.—have electronic devices embedded in most aspects of their systems, often providing critical controls. Electric power has thus emerged as an essential service underlying US society and all of its other critical infrastructures. Telecommunications has grown to a critical level but may not rise to the same level as electrical power in terms of risk to the Nation’s survival. All other infrastructures and critical functions are dependent upon the support of electric power and telecommunications. Therefore, we must make special efforts to prepare and protect these two high-leverage systems.





**Figure 4. Interdependent Infrastructure Sectors**

Most critical infrastructure system vulnerabilities can be reduced below the level that potentially invites attempts to create a national catastrophe. By protecting key elements in each critical infrastructure and by preparing to recover essential services, the prospects for a terrorist or rogue state being able to achieve large-scale, long-term damage can be minimized. This can be accomplished reasonably and expeditiously.

Such preparation and protection can be achieved over the next few years, given a dedicated commitment by the federal government and an affordable investment of resources. We need to take actions and allocate resources to decrease the likelihood that catastrophic consequences from an EMP attack will occur, to reduce our current serious level of vulnerability to acceptable levels and thereby reduce incentives to attack, and to remain a viable modern society even if an EMP attack occurs. Since this is a matter of national security, the federal government must shoulder the responsibility of managing the most serious infrastructure vulnerabilities.

*The most critical infrastructure system vulnerabilities can be reduced below those levels that invite attack or cause a national catastrophe.*

Homeland Security Presidential Directives 7 and 8 lay the authoritative basis for the Federal government to act vigorously and coherently to mitigate many of the risks to the Nation from terrorist attack. The effects of EMP on our major infrastructures lie



within these directives, and the directives specify adequate responsibilities and provide sufficient authorities to deal with the civilian sector consequences of an EMP attack.

In particular, the Department of Homeland Security (DHS) has been established, led by a Secretary with authority, responsibility, and the obligation to request needed resources for the mission of protecting the US and recovering from the impacts of the most serious threats. This official must assure that plans, resources, and implementing structures are in place to accomplish these objectives, specifically with respect to the EMP threat. In doing so, DHS must work in conjunction with the other established governmental institutions and with experts in the private sector to most efficiently accomplish this mission. It is important that metrics for assessing improvements in prevention, protection, and recovery be put in place and then evaluated and that progress be reported regularly. DHS must clearly and expeditiously delineate its responsibility and actions in relation to other governmental institutions and the private sector, in order to provide clear accountability and avoid confusion and duplication of effort.

Specific recommendations are provided below with respect to both the particulars for securing each of the most critical national infrastructures against EMP threats and the governing principles for addressing these issues of national survival and recovery in the aftermath of EMP attack.

## STRATEGY AND RECOMMENDATIONS

It will not be possible to reduce the incentives for an EMP attack to an acceptable level of risk through defensive protection measures alone. It is possible to achieve an acceptable level of risk and reduced invitation to an EMP attack with a strategy of:

- Pursuing intelligence, interdiction, and deterrence to discourage EMP attack against the US and its interests
- Protecting critical components of the infrastructure, with particular emphasis on those that, if damaged, would require long periods of time to repair or replace
- Maintaining the capability to monitor and evaluate the condition of critical infrastructures
- Recognizing an EMP attack and understanding how its effects differ from other forms of infrastructure disruption and damage
- Planning to carry out a systematic recovery of critical infrastructures
- Training, evaluating, “Red Teaming,” and periodically reporting to the Congress
- Defining the Federal Government’s responsibility and authority to act
- Recognizing the opportunities for shared benefits
- Conducting research to better understand infrastructure system effects and developing cost-effective solutions to manage these effects

The cost for such improved security in the next 3 to 5 years is modest by any standard—and extremely so in relation to both the war on terror and the value of the national infrastructures involved. Costs at later times may be adjusted to deal with the then-apparent threat and future levels of effort required.

### INTELLIGENCE, INTERDICTION, AND DETERRENCE

The federal government’s efforts to establish and maintain a global environment that profoundly discourages potentially catastrophic attacks is our first line of defense. The development, trading, and movement of critical materials and weapons useful for mounting WMD attacks, including those that are based on the use of EMP, must be identified as early in the process as possible. The methods and materials that could encourage an EMP attack must be added to the list of threats presently being sought out and annihilated. The US and its allies against transnational terrorism must make it

exceedingly difficult and dangerous for organizations to position themselves to be a threat, or allow others to use their country and its assets in order to become a threat, specifically including EMP threats. We must hold potential perpetrators at risk of capture or destruction, whenever and wherever in the world they operate.

#### PROTECTING CRITICAL COMPONENTS OF THE INFRASTRUCTURE

Some components of critical infrastructures, such as large turbines, generators, and high-voltage transformers in electrical power systems, and electronic switching systems in telecommunication systems, would require long periods of time to repair or replace. These components should be configured so that even under electronic disruption and damage, such as could be produced by EMP, they do not become further damaged in the course of shutting down or attempting to restore themselves. This type of damage has occurred in the past. During the Northeast power blackout of 1965, Consolidated Edison generators, transformers, motors, and auxiliary equipment were damaged by the sudden shutdown. In particular, the #3 unit at the Ravenswood power plant in New York City suffered damage when the blackout caused loss of oil pressure to the main turbine bearing. The damage kept that unit out of service for nearly a year, and more immediately, complicated and delayed the restoration of service to New York City.

#### MAINTAINING THE CAPABILITY TO MONITOR AND EVALUATE THE CONDITION OF CRITICAL INFRASTRUCTURES

After an EMP attack, system operators and others in positions of authority and responsibility must have immediate access to information sufficient to characterize the state of their critical infrastructure systems. Without such system monitoring and reporting information, the system operators will not have the information required to evaluate the extent of the loss of infrastructure and know how to begin restoration of their systems. They may even induce further damage by taking inappropriate actions or failing to take necessary actions. During the time leading up to the August 14, 2003, Midwest power blackout that affected both the United States and Canada, key system operators did not have a functioning alarm system, did not recognize that the alarm system was not functioning, and had only fragmentary information on the changing configuration of the rapidly collapsing power grid for which they were responsible.

#### RECOGNIZING EMP ATTACK

Electronic upsets and failures occur under normal operating circumstances, even in high-reliability equipment such as that supporting critical infrastructure. EMP-induced

upsets and failures, however, are different from those encountered in the normal operation of infrastructure systems, and in fact have unique aspects not encountered under any other circumstances.

EMP produces nearly simultaneous upset and damage of electronic and of other electrical equipment over wide geographic areas, determined by the altitude, character, and explosive yield of the EMP-producing nuclear explosion. Since such upset and damage is not encountered in other circumstances and particularly not remotely to the same scale, the normal experience of otherwise skilled system operators and others in positions of responsibility and authority will not have prepared them to identify what has happened to the system, what actions to take to minimize further adverse consequences, and what actions must be carried out to restore the impacted systems as swiftly and effectively as possible.

Special system capabilities and operator awareness, planning, training, and testing will be required to deal with EMP-induced system impacts. The first requirement is for the operators of critical infrastructure systems to be able to determine that a high-altitude nuclear explosion has occurred and has produced a unique set of adverse effects on their systems. That information can be provided by local electromagnetic sensors, by information from Earth satellite systems, or by other means. Whatever the means, the operators and others in positions of authority and responsibility must receive the information immediately. Therefore, the EMP event notification system must itself be highly reliable during and after an EMP attack.

Operators and others in positions of authority and responsibility must be trained to recognize that an EMP attack in fact has taken place, to understand the wide range of effects it can produce, to analyze the status of their infrastructure systems, to avoid further system degradation, to dispatch resources to begin effective system restoration, and to sustain the most critical functions while the system is being repaired and restored. Failures similar to those induced by EMP do not occur in normal system operation; therefore, the training for, and experience developed in the course of, normal system operation will not provide operators with the skills and knowledge base necessary to perform effectively after EMP-induced system disruption and failure. Training, procedures, simulations, and exercises must be developed and carried out that are specifically designed to contend with EMP-induced effects.

## PLANNING TO CARRY OUT A SYSTEMATIC RECOVERY OF CRITICAL INFRASTRUCTURES

A crisis such as the immediate aftermath of an EMP attack is not the time to begin planning for an effective response. Plans to avoid causing further damage to critical infrastructures and to carry out a systematic recovery of those infrastructures must be in hand at the earliest possible time. Planning for responding to an EMP attack should begin now and should be carried out jointly by system operators, hardware and software providers, and experts in both the government and private sectors.

Individual infrastructure systems have many similar electronically based control and monitoring functions. The primary features of EMP attack mitigation in each infrastructure include elements of protection of critical functions, identifying where damage within the system is located, dispatch/allocation of resources to allow for timely restoration and development of operational procedures including simulation of both individual and interacting infrastructures, training, testing, and governance. This requires test and evaluation of both existing and future systems to identify weak spots subject to EMP damage and focus mitigation activities accordingly. EMP protection thus has a substantial aspect focused on individual functioning units within each system that contains electronic components, although not necessarily on the individual electronic subcomponents of these units themselves. These units include distributed Supervisory Control and Data Acquisition (SCADA) modules, mobile communicators, radios, embedded control computers, etc. New units can be EMP-hardened for a very small fraction of the cost of the non-hardened item, e.g., 1% to 3% of cost, if hardening is done at the time the unit is designed and manufactured. In contrast, retrofitting existing functional components is potentially an order of magnitude more expensive and should be done only for critical system units. It is important to note, however, that for protection to remain functional, it must be tested and maintained in its operational mode with rigor and discipline.

## TRAINING, EVALUATING, RED TEAMING, AND PERIODICALLY REPORTING TO THE CONGRESS

Identifying an EMP attack, understanding the state of the system after attack, developing and implementing plans for system restoration, and having operators and others in positions of authority and responsibility trained to recognize and respond effectively are elements of strategy that are common to managing the effects of EMP for each of the Nation's critical infrastructure components. Conducting and evaluating the results of training, simulations, tests, and Red Team activities, and periodically reporting

the results to senior executive branch leaders, the Congress, and the public are important elements of being well-prepared for EMP attack, which in turn will sharply reduce the incentives for conduct of such an attack.

#### DEFINING THE FEDERAL GOVERNMENT’S RESPONSIBILITY AND AUTHORITY TO ACT

Governance of the critical infrastructures such as electrical power systems and communications is presently distributed among statutory governmental entities at the federal, state, regional, and municipal levels, as well as among a variety of non-governmental entities. A multiplicity of statutory bodies, private companies, associations, and individual owners also participate in determining decisions and actions. Nevertheless, the process is coordinated, albeit loosely, to produce normal efficient, reliable, and high quality service that is the envy of the world—in a peacetime environment.

A terrorist threat—let alone a terrorist attack—is outside the ambit of normal governance of the key national infrastructures. In dealing with such threats, the Department of Homeland Security has the unique and sole responsibility and authority to govern the specific actions and involved parties within the US, including requesting enabling Congressional funding as appropriate and necessary. DHS must interact with other governmental institutions and the private sector in defining liability, responsibility and funding in order to enable private and government facilities, such as independent power plants, to contribute their capability in a time of national need, yet not interfere with market creation and operation to the maximum extent practical.

***DHS must interact with other governmental institutions and the private sector in defining liability, responsibility, and funding in order to enable private and government facilities, such as independent power plants, to contribute their capability in a time of national need, yet not interfere with market creation and operation to the maximum extent practical.***

Industry associations, system owners/providers, private consultants, and universities all will be able to contribute useful levels of knowledge and skills. DHS is responsible for making the prudent trade-offs within each mitigation activity between performance, risk, schedule, and cost in relation to consequent system protection and then-expected risk in order to achieve maximum protection. For example, some actions taken to protect a system from an EMP attack may diminish the reliability or quality of that system’s normal commercial performance, while other actions may improve the performance.



As an example of resources readily available to DHS with respect to the electric system, the North American Reliability Counsel (NERC) and the Electric Power Research Institute are well-positioned to provide much of the support needed in regard to the EMP threat. Working closely with industry and these institutions, the DHS should provide for the necessary capability to control the national bulk electricity supply system in order to protect critical services, minimize its self-destruction in the event of an EMP attack, and recover its normal capabilities as rapidly and effectively as possible thereafter.

#### RECOGNIZING THE OPPORTUNITIES FOR SHARED BENEFITS

Most of the following initiatives and actions the Commission recommends militate against more than an EMP attack. The protection and/or rapid restoration of critical infrastructures in the civilian sector from an EMP attack also will be effective against other types of infrastructure disruptions, such as attacks aimed at directly damaging or destroying key components of the electrical system, and natural or accidental large-scale disruptions are also significantly mitigated by these same initiatives. Some of these steps also enhance reliability and quality of critical infrastructures, which is a major direct benefit to the US economy and to our way of life.

#### CONDUCTING RESEARCH AND DEVELOPMENT

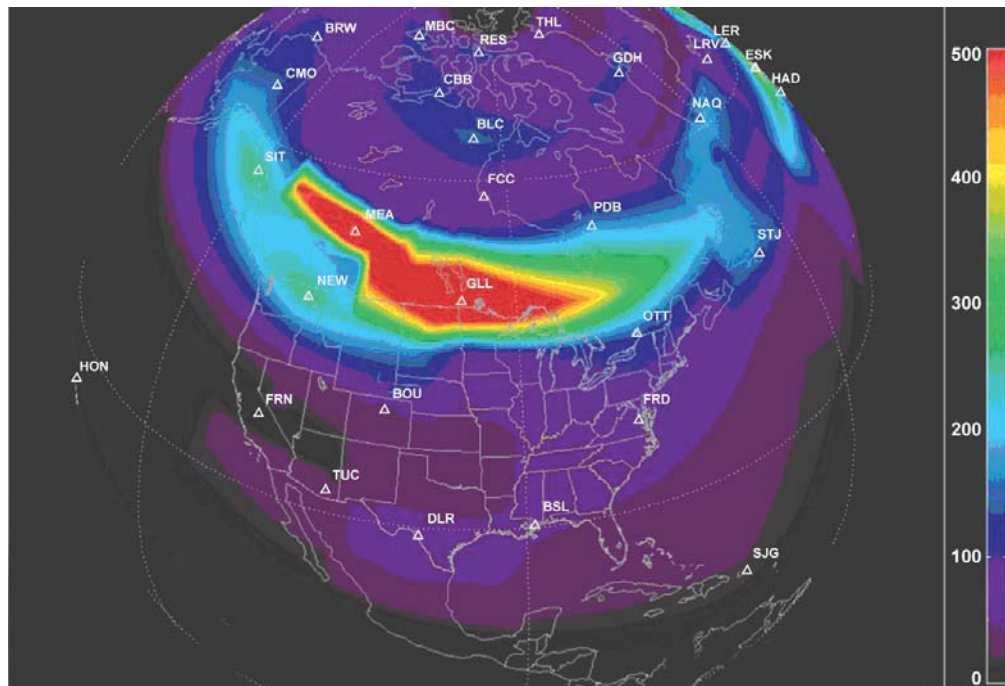
Very little research and development addressing EMP-related system response protection and recovery issues has been done for more than a decade. Conducting research to better understand infrastructure system effects and developing cost-effective solutions to manage these effects will be important to understanding the implications of the rapid evolution of electronics and electrical systems, and their growing role in controlling and operating modern critical infrastructure.

## ELECTRIC POWER INFRASTRUCTURE

### NATURE OF THE PROBLEM

Electric power is integral to the functioning of electronic components. For highly reliable systems such as commercial and military telecommunications, electric power usually comes from batteries (in the short term), local emergency power supplies (generally over time-intervals of less than 72 hours), and electricity delivered through the local electrical utility (“power” lines in the home, office and factory). Local emergency power supplies are limited by supplies of stored fuel. Increasingly, locally stored fuel in buildings and cities is being reduced for fire safety and environmental pollution reasons, so that the emergency generation availability without refueling is limited.

Geomagnetic storms, a natural phenomenon driven by the solar wind, may, by a different physical mechanism, produce ground-induced currents (GIC) that can affect the electrical system in a manner similar to the E3 component of EMP. Disruptions caused by geomagnetic storms, such as the collapse of Quebec Hydro grid during the geomagnetic storm of 1989, have occurred many times in the past (Figure 5).



Geomagnetic field disturbance conditions, dB/dt (nT/min) over North America at time 7:45 UT on March 13, 1989

Source: Metatech Corporation, Applied Power Solutions

**Figure 5. Extent of 1989 Geomagnetic Storm**

Depending on the explosive yield of the nuclear weapon used, EMP-induced GIC may be several times larger than that produced by the average geomagnetic storm, and may even be comparable to those expected to arise in the largest geomagnetic storm ever observed. It may also occur over an area not normally affected by historic geomagnetic storms.

The North American economy and the functioning of the society as a whole are critically dependent on the availability of electricity, as needed, where and when needed. The electric power system in the US and interconnected areas of Canada and Mexico is outstanding in terms of its ability to meet load demands with high quality and reliable electricity at reasonable cost. However, over the last decade or two, there has been relatively little large-capacity electric transmission constructed and the generation additions that have been made, while barely adequate, have been increasingly located considerable distances from load for environmental, political, and economic reasons. As a result, the existing National electrical system not infrequently operates at or very near local limits on its physical capacity to move power from generation to load. Therefore, the slightest insult or upset to the system can cause functional collapse affecting significant numbers of people, businesses, and manufacturing. It is not surprising that a single EMP attack may well encompass and degrade at least 70% of the Nation's electrical service, all in one instant.

The impact of such EMP is different and far more catastrophic than that effected by historic blackouts, in three primary respects:

1. The EMP impact is virtually instantaneous and occurs simultaneously over a much larger geographic area. Generally, there are neither precursors nor warning, and no opportunity for human-initiated protective action. The early-time EMP component is the "electromagnetic shock" that disrupts or damages electronics-based control systems and sensors, communication systems, protective systems, and control computers, all of which are used to control and bring electricity from generation sites to customer loads in the quantity and quality needed. The E1 pulse also causes some insulator flashovers in the lower-voltage electricity distribution systems (those found in suburban neighborhoods, in rural areas and inside cities), resulting in immediate broad-scale loss-of-load. Functional collapse of the power system is almost definite over the entire affected region, and may cascade into adjacent geographic areas.
2. The middle-time EMP component is similar to lightning in its time-dependence but is far more widespread in its character although of lower amplitude—essentially a great many lightning-type insults over a large geographic area which might obviate protection. The late-time EMP component couples very efficiently

to long electrical transmission lines and forces large direct electrical currents to flow in them, although they are designed to carry only alternating currents. The energy levels thereby concentrated at the ends of these long lines can become large enough to damage major electrical power system components. The most significant risk is synergistic, because the middle and late-time pulses follow after the early-time pulse, which can impair or destroy protective and control features of the power grid. Then the energies associated with the middle and late-time EMP thus may pass into major system components and damage them. It may also pass electrical surges or fault currents into the loads connected to the system, creating damage in national assets that are not normally considered part of the infrastructure per se. Net result is recovery times of months to years, instead of days to weeks.

3. Proper functioning of the electrical power system requires communication systems, financial systems, transportation systems, and—for much of the generation—continuous or nearly continuous supply of various fuels. However, the fuel-supply, communications, transportation, and financial infrastructures would be simultaneously disabled or degraded in an EMP attack and are dependent upon electricity for proper functioning. For electrical system recovery and restoration of service, the availability of these other infrastructures is essential. The longer the outage, the more problematic, and uncertainty-fraught the recovery will be.

The recent cascading outage of August 14, 2003, is an example of a single failure compounded by system weaknesses and human mistakes. It also provides an example of the effectiveness of protective equipment. However, with EMP there are multiple insults coupled with the disabling of protective devices simultaneously over an extremely broad region—damage to the system is likely and recovery slow.

#### RECOMMENDED MITIGATION AND RESPONSIBILITY

The electrical system is designed to break into “islands” of roughly matching generation and load when a portion of the system receives a severe electrical insult. This serves both to protect electricity supply in the non-impacted regions and to allow for the stable island-systems to be used to “restart” the island(s) that have lost functionality. With EMP, the magnitude, speed, and multi-faceted nature of the insult, its broad geographic reach, along with the number of simultaneous insults, and the adverse synergies all are likely to result in a situation where the islanding scheme will fail to perform as effectively as intended, if at all. Since the impacted geographic area is large, restoring the system from the still-functioning perimeter regions would take a great deal of time, possibly weeks to months at best. Indeed, the only practical way to restart much of the impacted electrical system may be with generation that can be started without an external power source. This is called “black start” generation and primarily includes

hydroelectric (including pumped storage), geothermal, and independent diesel generators of modest capacity.

The recommended actions will substantially improve service and recovery during “normal” large-scale blackouts, and will critically enable recovery under EMP circumstances.

#### PROTECTION

It is impractical to protect the entire electrical power system from damage by an EMP attack. There are too many components of too many different types, manufacturers, designs, and vulnerabilities within too many jurisdictional entities, and the cost to retrofit is too great. Widespread functional collapse of the electrical power system in the area affected by EMP is possible in the face of a geographically broad EMP attack, with even a relatively few unprotected components in place. However, it is practical to reduce to low levels the probability of widespread damage to major power system components that require long times to replace. This will enable significantly improved recovery times, since it avoids the loss of long lead-time and critical components. It is important to protect the ability of the system to fragment gracefully into islands, to the extent practical in the particular EMP circumstance. This approach is cost-efficient and can leverage efforts to improve reliability of bulk electricity supply and enhance its security against the broader range of threats.

***Widespread functional collapse of the electric power system in the area affected by EMP is likely.***

#### RESTORATION

The key to minimizing adverse effects from loss of electrical power is the speed of restoration. Restoration involves matching generation capacity to a load of equivalent size over a transmission network that is initially isolated from the broader system. The larger system is then functionally rebuilt by bringing that mini system, or “island,” to the standard operating frequency and thereupon by adding more blocks of generation and load to this core in amounts that can be absorbed by the growing subsystem. This is a demanding and time-consuming process in the best of circumstances. In the singular circumstance of an EMP attack with multiple damaged components, related infrastructure failures, and particularly severe challenges in communications and transportation, the time required to restore electrical power is expected to be considerably longer than we have experienced in recent history.

However, by protecting key system components needed for restoration, by structuring the network to fail gracefully, and by creating a comprehensive prioritized recovery plan for the most critical power needs, the risk of an EMP attack having a catastrophic effect on the Nation can be greatly reduced. DHS must ensure that the mitigation plan is jointly developed by the federal government and the electric power industry, implemented fully, instilled into systems operations, and tested and practiced regularly to maintain a capability to respond effectively in emergencies. The North American Reliability Council and the Electric Power Research Institute are aptly positioned to provide much of what's needed to support DHS in carrying out its responsibilities. The US Energy Association is well-suited to coordinating activities between and among the various energy sectors that together affect the electric power system and its vitality.

#### ESSENTIAL COMPONENT PROTECTION

1. Assure protection of high-value long-lead-time transmission assets.
2. Assure protection of high-value generation assets. System-level protection assurance is more complex due to the need for multiple systems to function in proper sequence.
3. Assure Key Generation Capability. Not all plants can or should be protected. However, regional evaluation of key generating resources necessary for recovery should be selected and protected.
  - a. Coal-fired generation plants make up nearly half the Nation's generation and are generally the most robust overall to EMP, with many electromechanical controls still in operation. Such coal plants also normally have at least a few days to a month of on-site fuel storage.
  - b. Natural gas-fired combustion turbines and associated steam secondary systems represent the newest and a significant contributor to meeting loads. These have modern electronics-based control and thus are more vulnerable. Natural gas is not stored on-site and likely will be interrupted in an EMP attack. However, provision can be made to have gas-fired plants also operate on fuel oil; many do already.
  - c. Nuclear plants produce roughly 20% of the Nation's generation and have many redundant fail-safe systems that tend to remove them from service whenever any system upset is sensed. Their safe shut down should be assured, but they will be unavailable until near the end of restoration.
  - d. Hydroelectric power is generally quite robust to EMP, and constitutes a substantial fraction of total national generation capacity, albeit unevenly distributed geographically.



- e. In general, the various distributed and renewable fueled generators are not significant enough at this time to warrant special protection.
  - f. Black start generation of all types is critical and will need to be protected from EMP upset or damage.
4. Assure functional integrity of critical communications channels. The most critical communications channels in the power grid are the ones that enable recovery from collapse, such as ones that enable manual operation and coordination-supporting contacts between distant system operators and those that support system diagnostics. Generation, switching, and load dispatch communications support is next in importance.
  5. Assure availability of emergency power at critical facilities needed for restoration. Transmission substations need uninterruptible power to support rapid restoration of grid connectivity and operability, and thereby to more quickly restore service. Most have short-life battery backup systems, but relatively few have longer-duration emergency generators; much more emphasis on the latter is needed.
  6. Assure protection of fuel production and its delivery for generation. Fuel supply adequate to maintain critical electrical service and to restore expanded service is critical. See Fuel/Energy Infrastructure, page 35) for details.
  7. Expand and assure intelligent islanding capability. The ability of the larger electrical power system to break into relatively small subsystem islands is important to mitigate overall EMP impacts and provide faster restoration.
  8. Develop and deploy system test standards and equipment. Device-level robustness standards and test equipment exist, but protection at the system level is the overarching goal. System-level robustness improvements such as isolators, line protection, and grounding improvements will be the most practical and least expensive in most cases relative to replacement with more robust individual component devices. Periodic testing of system response is necessary.

## SYSTEM RESTORATION

1. Develop and enable a restoration plan. This plan must prioritize the rapid restoration of power to government-identified critical service. Sufficient black start generation capacity must be provided where it is needed in the associated subsystem islands, along with transmission system paths that can be isolated and connected to matching loads. The plan must address outages with wide geographic coverage, multiple major component failures, poor communication capabilities, and widespread failure of islanding schemes within the EMP-affected area. Government and industry responsibilities must be unequivocally and completely assigned. All necessary legal and financial arrangements, e.g., for indemnification, must be put into place to allow industry to implement specified government priorities with respect to service restoration, as well as to deal with potential environmental and technical hazards in order to assure rapid recovery.

2. Simulate, train, exercise, and test the plan. Simulators must be developed for use in training and developing procedures similar to those in the airline industry; a handful should suffice for the entire country. Along with simulation and field exercises, Red Team discipline should be employed to surface weaknesses and prioritize their rectification.
3. Assure sufficient numbers of adequately trained recovery personnel.
4. Assure availability of replacement equipment. R&D is under way—and should be vigorously pursued—into the production of emergency “universal” replacements. The emergency nature of such devices would trade efficiency and service-life for modularity, transportability, and affordability.
5. Implement redundant backup diagnostics and communication. Assure that system operators can reliably identify and locate damaged components.

## TELECOMMUNICATIONS

### IMPORTANCE OF ASSURED TELECOMMUNICATIONS

Telecommunications plays a key role in US society in terms of its direct effect on individuals and business and due to its impact on other key infrastructures. The relationship of telecommunications to the other critical infrastructures, such as the financial industry, is often recognized during and following widespread outages, such as those experienced as a result of the September 11, 2001, attacks on the World Trade Centers and the immediate vicinity of “Ground Zero.” The local disruption of all critical infrastructures, including power, transportation, and telecommunications, interrupted operations in key financial markets and posed increased liquidity risks to the US financial system.<sup>1</sup> In the days following the attacks, institutions in the affected areas were implementing their business continuity plans, which proved vital to the rapid restoration and recovery of services in the New York City area. In addition, the President emphasized that the prompt restoration of Wall Street’s capabilities was critical to the economic welfare of the Nation; in doing so, he aptly linked economic stability to national security.

For some of the most critical infrastructure services, such as electric power, natural gas, and financial services, assured communications are essential to their recovery following a major adverse event. The importance of telecommunications in an emergency situation is underscored by the existence of the National Communications System (NCS), established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*,<sup>2</sup> which include administering the National

---

<sup>1</sup> James J. MacAndrews and Simmon M. Potter, “Liquidity Effects of the Events of September 11, 2001,” Federal Reserve Bank of New York Economic Policy Review, November 2002.

<sup>2</sup> The mission of the NCS shall be to assist the President, the National Security Council, the Homeland Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget in: (1) the exercise of the telecommunications functions and responsibilities set forth in Section 2 of this Order; and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.

The NCS shall seek to ensure that a national telecommunications infrastructure is developed which: (1) Is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies and other entities, including telecommunications in support of national security leadership and continuity of government; (2) Is capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources; (3) Incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain, to the maximum extent

Coordinating Center (NCC) for Telecommunications to facilitate the initiation, coordination, restoration, and reconstitution of National Security and Emergency Preparedness (NS/EP) telecommunications services or facilities under all crises and emergencies; developing and ensuring the implementation of plans and programs that support the viability of telecommunications infrastructure hardness, redundancy, mobility, connectivity, and security; and serving as the focal point for joint industry-government and interagency NS/EP telecommunications planning and partnerships. In addition, the President's National Security Telecommunications Advisory Committee (NSTAC), a Federal Advisory Committee Act (FACA) CEO-level advisory group to the President, is tasked with providing industry-sourced advice and expertise related to implementing policies affecting NS/EP communications. These NS/EP services are those "critical to the maintenance of a state of readiness or the response to and management of any event or crisis that causes harm or could cause harm to the population, damage to or the loss of property, or degrades or threatens the NS/EP posture of the United States."<sup>3</sup>

The NSTAC in its 1985 Report on EMP found that "consistent with its cost constraints, industry should incorporate low-cost EMP mitigation practices into new facilities and, as appropriate, into upgrade programs. For those areas where a carrier/supplier recognizes that a significant improvement in EMP resistance and surveillance could be achieved, but at a cost beyond the carrier/supplier's own cost constraints, the carrier/supplier should identify such options to the government for evaluation and possible funding." On October 9, 1985, the NSTAC approved the EMP Final Task Force Report and forwarded a recommendation to the President, calling for a joint industry and Government program to reduce the costs of existing techniques for mitigating high-altitude electromagnetic pulse (HEMP)-induced transients and to develop new techniques for limiting transient effects. As a result, the NCS and industry, working with the ATIS—the Alliance for Industry Solutions—developed a set of ANSI standards and Generic Requirements<sup>4</sup> to address EMP.<sup>5</sup>

---

practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency; and (4) Is consistent, to the maximum extent practicable, with other national telecommunications policies.

<sup>3</sup> NS/EP Implications for Electronic Commerce, NSTAC Report, June 1999.

<sup>4</sup> Telcordia GR-1089-CORE.

<sup>5</sup> ANSI T1.320.

### NS/EP Definitions

***NS/EP Telecommunications Services:*** Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrades or loss of property, or degrades or threatens the NS/EP posture of the United States. (*“Telecommunications Service Priority [TSP] System for National Security Emergency Preparedness: Service User Manual,” NCS Manual 3-1-1, July 9, 1990. Appendix A.*)

***NS/EP Requirements:*** Features that maintain a state of readiness or respond to and manage an event or crisis (local, national, or international), which causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the NS/EP posture of the United States. (*Federal Standard 1037C*)

With respect to NS/EP telecommunications, capabilities exist for prioritizing phone calls through the wireline, wireless, and satellite networks during the time interval when call volumes are excessive and facilities are damaged, giving priority to restoring services that may be damaged or degraded, and getting new circuits into operation.

According to recent testimony by a DHS official, “The NCS is continuing a diverse set of mature and evolving programs designed to ensure priority use of telecommunications services by NS/EP users during times of national crisis. The more mature services—including the Government Emergency Telecommunications Service (GETS) and the Telecommunications Service Priority (TSP)—were instrumental in the response to the September 11 attacks. FY 2005 funding enhances these programs and supports the development of the Wireless Priority Service (WPS) program and upgrade to the Special Routing Arrangement Service (SRAS). Specifically, priority service programs include: (1) GETS, which offers nationwide priority voice and low-speed data service during an emergency or crisis situation; (2) WPS, which provides a nationwide priority cellular service to key NS/EP users, including individuals from federal, state and local governments and the private sector; (3) TSP, which provides the administrative and operational framework for priority provisioning and restoration of critical NS/EP telecommunications services; (4) SRAS, which is a variant of GETS to support the Continuity of Government (COG) program including the reengineering of SRAS in the AT&T network and development of SRAS capabilities in the MCI and Sprint networks, and; (5) the Alerting and Coordination Network (ACN), which is an NCS program that

provides dedicated communications between selected critical government and telecommunications industry operations centers.”<sup>6</sup>

For example, due to concerns with respect to getting calls through during intervals of high network call volumes that follow disaster events, the Nuclear Regulatory Commission (NRC) utilizes the Government Emergency Telecommunications System (GETS) and other NS/EP telecom services such as wireless priority services to communicate with commercial nuclear power plants and to relay critical status information. This use of GETS grew out of lessons learned from the Three Mile Island incident in 1979. During the initial days of this incident, NRC personnel experienced communication problems that were attributed primarily to call volume overload at the local telephone company switch.

Another NS/EP service is the Telecommunications Service Priority (TSP) program, which exists to assign priority provisioning and restoration of critical NS/EP telecommunications services in the hours immediately following a major disaster. In place since the mid-1980s, more than 50,000 circuits are protected today under TSP, including circuits associated with critical infrastructures such as electric power, telecommunications, and financial services.

The telecommunication system consists of four basic and primary physical systems: wireline, wireless, satellite, and radio. In general, the national telecommunications infrastructure may be farther advanced than others in its ability to address the particular consequences of EMP. This is due in large measure to the recognized alternative threats to this system, as well as broad recognition of its importance to society. The three primary and separate systems (excluding radio) that make up the broad telecommunications infrastructure each provide specialized services; they also overlap heavily. Thus the loss or degradation of any one of these somewhat redundant subsystems subjects the remaining functional subsystems to heavier service loads.

Each of these four primary systems is unique in their capability to suffer insult from EMP. The wireline system is robust but will be degraded within the area exposed to the EMP electromagnetic fields. The wireless system is technologically fragile in relation

---

<sup>6</sup> Statement of General Frank Libutti, Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, Before the House Homeland Select Subcommittee on Intelligence and Counterterrorism and the Subcommittee on Infrastructure and Border Security, March 4, 2004, p. 12.



to EMP, certainly in comparison to the wireline one. In general, it may be so seriously degraded in the EMP region as to be unavailable. Low Earth Orbit (LEO) communications satellites may also suffer radiation damage as a result of one or more high-altitude nuclear bursts that produce EMP (see Space Systems, page 44).

The radio communication sub-system of the national telecommunications infrastructure is not widespread, but where it is connected to antennas, power lines, telephone lines, or other extended conductors, it is also subject to substantial EMP damage. However, radio communication devices not so connected or not connected to such conductors at the time of the EMP attack are likely to be operable in the post-attack interval.

#### EMP EFFECTS ON TELECOMMUNICATIONS

Based upon results of Commission-sponsored testing, an EMP attack would disrupt or damage a functionally significant fraction of the electronic circuits in the Nation's civilian telecommunications systems in the region exposed to EMP. The remaining operational networks would be subjected to high levels of call attempts for some period of time after the attack, leading to degraded telecommunications services.

Key government and civilian personnel will need priority access to use public network resources to coordinate and support local, regional, and national recovery efforts, especially during the interval of severe network congestion.

To offset the temporary loss of electric power, telecommunications sites now utilize a mix of batteries, mobile generators, and fixed-location generators. These typically have between 4 and 72 hours of backup power available, and thus will depend on either the resumption of electrical utility power or fuel deliveries to function for longer periods of time.

For some of the most critical infrastructure services such as electric power, natural gas, and financial services, assured communications are necessary—but aren't necessarily sufficient—to the survival of that service during the initial time-intervals after an EMP attack. Therefore, a systematic approach to protecting or restoring key communications systems will be required.

#### RECOMMENDED MITIGATION ACTIVITIES

The following actions are recommended as particularly effective ones for mitigating the impacts of EMP attack:

- Expand the respective roles of the National Communications System (NCS) and the Defense Threat Reduction Agency (DTRA) as the Federal Focal Point for EMP within the Code of Federal Regulations Part 215<sup>7</sup> to address infrastructure interdependencies related to NS/EP telecommunications services.
- Ensure services targeted at NS/EP operate effectively as new technology is introduced into the telecommunications network. Specifically, services such as Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) that are intended for use in emergency situations to improve the call completion probabilities for key personnel must operate effectively. Within the next 15 years, new technologies will be introduced into the public networks that will play major roles in operation of these services. EMP is just one of the potential threats that could stress the telecommunications networks; therefore, ensuring that NS/EP services perform effectively as new technology is introduced has benefits beyond providing robustness to EMP, and moreover is consistent with avoiding failures from other hostile actions.
- Determine the effects of EMP on different types of telecommunication equipment and facilities, using tests and theoretical analyses of the type done in the course of Commission-sponsored work and previous EMP-related studies conducted by the National Communications System (NCS).<sup>8</sup> A comprehensive, continuing telecommunications testing program,<sup>9</sup> along with the use of existing national and international standards,<sup>10</sup> may be a model activity that would be a key part of this overall National effort.
- Improve the ability of key network assets to survive HEMP. There are key elements in the network such as the Signal Transfer Points (STPs) in the signaling system (Signaling System 7 (SS7)), Home Location Register (HLR), and Visiting Location Register (VLR) in the wireless networks whose degradation can result in the loss of service to a larger number of users. Effective mitigation strategies include a combination of site hardening and installation of protective measures for the fast rise-time (E1) component of EMP.
- Improve the ability of telecommunications to withstand the sustained loss of utility-supplied electric power. This mitigation strategy would entail the use of best practices, review and improvement of existing programs such

---

<sup>7</sup> 47CFR, Section 215, designated The Executive Agent, NCS, is the focal point within the Federal Government for all EMP technical data and studies concerning NS/EP telecommunications.

<sup>8</sup> For example: The Effects of High-Altitude Electromagnetic Pulse (HEMP) on Telecommunications Assets, NCS Technical Information Bulletin 92-5, February 1992.

<sup>9</sup> Similar to that conducted in response to the Signaling System 7 outages of the early 1990's (which affected large portions of the United States) under the Inter-network Interoperability Test Program (IITP) of the Alliance for Telecommunications Industry Solutions (ATIS).

<sup>10</sup> Standards for Protection of Telecommunications Links, NCS Technical Notes, Volume 6, Number 3, 1999.

as the Telecommunications Electric Service Priority (TESP) program, and the increased use of alternative backup power sources.

- Conduct exercises to refine contingency operations. Conduct exercises that test and provide for improved contingency operations, assuming widespread multi-infrastructure degradation. The adequacy of mutual aid agreements, cross-organizational planning and coordination, and critical asset prioritization are examples of elements that should be tested and developed.
- Managers of these critical services must design their systems and operating procedures to take into account the potential vulnerabilities introduced by EMP-driven failure of telecommunications devices and sub-systems.

## BANKING AND FINANCE

### NATURE OF THE PROBLEM

The financial services industry comprises a network of organizations and attendant systems that process instruments of monetary value in the form of deposits, loans, funds transfers, savings, and other financial transactions. It includes banks and other depository institutions, including the Federal Reserve System; investment-related companies such as underwriters, brokerages, and mutual funds; industry utilities such as the New York Stock Exchange, the Automated Clearing House, and the Society for Worldwide Interbank Financial Telecommunications; and third party processors that provide electronic processing services to financial institutions, including data and network management and check processing.

Virtually all American economic activity depends upon the functioning of the financial services industry. Today, most financial transactions that express National wealth are performed and recorded electronically. Virtually all transactions involving banks and other financial institutions happen electronically. Essentially all record-keeping of financial transactions involves information stored electronically. The financial services industry has evolved to the point that it would be impossible to operate without the efficiencies, speeds, and processing and storage capabilities of electronic information technology.

The terrorist attacks of September 11, 2001, demonstrated the vulnerabilities arising from the significant interdependencies of the Nation's critical infrastructures. The attacks disrupted all critical infrastructures in New York City, including power, transportation, and telecommunications. Consequently, operations in key financial markets were interrupted, increasing liquidity risks for the United States financial system.<sup>11</sup>

The Interagency Paper,<sup>12</sup> which was jointly issued by the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), and the Securities and Exchange Commission (SEC), specifies clearing and settlement systems as the most

<sup>11</sup> James J. MacAndrews and Simmon M. Potter, "Liquidity Effects of the Events of September 11, 2001," Federal Reserve Bank of New York Economic Policy Review, November 2002.

<sup>12</sup> The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System*, September 5, 2002.

critical business operations at risk for financial markets.<sup>13</sup> Because financial markets are highly interdependent, a wide-scale disruption of core clearing and settlement processes would have an immediate systemic effect on critical financial markets.<sup>14</sup>

*Over the past couple of decades, the American economy has become increasingly resilient to shocks. Deregulated financial markets, far more flexible labor markets, and, more recently, the major advances in information technology have enhanced our ability to absorb disruptions and recover. In the past, our economy has quickly regained its previous levels following the devastation of hurricanes, earthquakes, floods, and myriad other natural disasters that periodically batter various regions of our country. Although the trauma of September 11 shares some characteristics with such disruptions, the differences are important. In contrast to natural disasters, last week's events are of far greater concern because they strike at the roots of our free society, one aspect of which is our market-driven economy. All modern economies require the confidence that free-market institutions are firmly in place and that commitments made today by market participants will be honored not only tomorrow, but for years into the future. The greater the degree of confidence in the state of future markets, the greater the level of long-term investment. The shock of September 11, by markedly raising the degree of uncertainty about the future, has the potential to result, for a time, in a pronounced disengagement from future commitments. And that, in the short run, would imply a lessened current level of activity. Indeed, much economic activity ground to a halt last week. But the foundations of our free society remain sound, and I am confident that we will recover and prosper as we have in the past. As a consequence of the spontaneous and almost universal support that we received from around the world, an agreement on a new round of multilateral trade negotiations now seems more feasible. Such an outcome would lead to a stronger global market system. A successful round would not only significantly enhance world economic growth but also answer terrorism with a firm reaffirmation of our commitment to open and free societies.*

—Testimony of Chairman Alan Greenspan, *The condition of the financial markets* Before the Committee on Banking, Housing, and Urban Affairs, US Senate September 20, 2001

Moreover, in December 2002, the FRB revised its policy and procedures for NS/EP telecommunications programs administered by the National Communications System (NCS) to identify those functions supporting the Federal Reserve's NS/EP mission to maintain national liquidity.<sup>15</sup> The FRB expanded the scope of services that would seriously affect continued financial operations if a telecommunications disruption

<sup>13</sup> Ibid., pg. 5.

<sup>14</sup> Systemic risk includes the risk that the failure of one participant in a transfer system or financial market to meet its required obligations will cause other participants to be unable to meet their obligations when due, causing significant liquidity or credit problems or threatening the stability of financial markets. The use of the term "systemic risk" in this report is based on the international definition of systemic risk in payments and settlement systems provided in Committee on Payment and Settlement Systems, Bank for International Settlements, "A Glossary of Terms in Payment and Settlement Systems," 2001.

<sup>15</sup> *Federal Register*, vol. 67, no. 236, Monday, December 9, 2002. Notice, "Federal Reserve Board Sponsorship for Priority Telecommunication Services of Organizations That Are Important to National Security/ Emergency Preparedness," <http://www.federalreserve.gov/boarddocs/press/other/2002/20021203/attachment.pdf>.

of “a few minutes to one day” occurred.<sup>16</sup> These functions, which are listed below, require same-day recovery and are critical to the operation and liquidity of banks and the stability of financial markets:

- Large-value inter-bank funds transfer, securities transfer, or payment-related services, such as Fedwire, Clearing House Interbank Payments System (CHIPS), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT)
- Automated clearinghouse (ACH) operators
- Key clearing and settlement utilities
- Treasury automated auction and processing system
- Large-dollar participants of these systems and utilities

The increasing dependence of the United States on an electronic economy, so beneficial to the creation and preservation of wealth, also adds to the adverse effects that would be produced by an EMP attack. The electronic technologies that are the foundation of the financial infrastructure are potentially vulnerable to EMP. These systems are also potentially vulnerable to EMP indirectly through other critical infrastructures, such as the electric power grid and telecommunications.

#### RECOMMENDED MITIGATION AND RESPONSIBILITY

Securing the financial services industry from the EMP threat is vital to the national security of the United States. The Federal government must assure that this system can survive sufficiently to preclude serious, long-term consequences.

The Department of Homeland Security, the Federal Reserve Board, and the Department of the Treasury, in cooperation with other relevant agencies, must develop contingency plans to ride out and recover key financial systems promptly from an EMP attack.

Key financial services include those means and resources that provide the general population with cash, credit, and other liquidity required to buy food, fuel, and other essential goods and services. We must protect the Nation’s financial networks, banking records, and data retrieval systems that support cash, check, credit, debit, and other transactions through judicious balance of hardening, redundancy, and contingency plans.

---

<sup>16</sup> Federal Reserve Board Sponsorship for Priority Telecommunications Services of Organizations That Are Important to National Security/Emergency Preparedness, *Federal Register*, Vol. 67, No. 236, Monday, December 2003, Notices, p. 72958.



The Federal government must work with the private sector to assure the protection and effective recovery of essential financial records and services infrastructure components from all deliberate adverse events, including EMP attack. Implementation of the recommendations made by the Department of the Treasury, the FRB, and the SEC in their *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System* to meet sabotage and cyber-threats that could engender requirements for protection and recovery should be expanded to include expeditious recovery from EMP attack:

- “Every organization in the financial services industry should identify all clearing and settlement activities in each critical financial market in which it is a core clearing and settlement organization or plays a significant role” that could be threatened by EMP attack.
- Industry should “determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets” following an EMP attack.
- Industry should be prepared to cope with an EMP attack by maintaining “sufficient geographically dispersed resources to meet recovery and resumption objectives.... Backup sites should not rely on the same infrastructure components (e.g., transportation, telecommunications, water supply, electric power) used by the primary site. Moreover, the operation of such sites should not be impaired by a wide-scale evacuation at or inaccessibility of staff that service the primary site.”
- Industry should, “Routinely use or test recovery and resumption arrangements.... It is critical for firms to test backup facilities of markets, core clearing and settlement organizations, and third-party service providers to ensure connectivity, capacity, and the integrity of data transmission” against an EMP attack.

## FUEL/ENERGY INFRASTRUCTURE

The vulnerabilities of this sector are produced by the responses of the electronic control systems that provide and utilize the near-real-time data flows needed to operate the fuel/energy infrastructure efficiently, as well as to identify and quickly react to equipment malfunctions or untoward incidents. EMP could also cause control or data-sensor malfunctions that are not easily discernible, leading to counterproductive operational decisions. Process control systems are critical to the operation and control of petroleum refineries, and little or no notice of an outage significantly increases the potential for damage during an emergency shutdown. Communications systems that are critical for operational control represent another locus of vulnerability. Communications are also critical in refineries to ensure safety of on-site personnel, the adjacent population, and the surrounding environment. The energy distribution infrastructure is also critically dependent on the availability of commercial power to operate the numerous pumps, valves and other electrical equipment that are required for a functional infrastructure.

DHS must develop a contingency plan that will provide strategy for protection and recovery for this sector, to include actions to be taken by both Government and industry. Government should establish a national inventory of parts for those items with long lead-times or that would be in demand in the event of a catastrophic event such as an EMP attack. The Energy Information Sharing and Analysis Center (ISAAC) should, with government funding, expand its mission to address EMP issues, and the government should work with the private sector to implement the general approach described in Strategy and Recommendations, page 11.

## TRANSPORTATION INFRASTRUCTURE

### NATURE OF THE PROBLEM

America's transportation sector is often addressed as a single infrastructure, but in reality its multiple modes provide for several separate infrastructures. Rail includes the freight railroad and commuter rail infrastructures; road includes the trucking and automobile infrastructures; water includes the maritime shipping and inland waterway infrastructures; and air includes the commercial and general aviation infrastructures.

As recognized by the President's National Security Telecommunications Advisory Committee (NSTAC) Information Infrastructure Group Report:<sup>17</sup>

- The transportation industry is increasingly reliant on information technology and public information-transporting networks.
- Although a nationwide disruption of the transportation infrastructure may be unlikely, even a local or regional disruption could have a significant impact. Due to the diversity and redundancy of the US transportation system, the infrastructure is not at risk of nationwide disruption resulting from information system failure. Nonetheless, a disruption of the transportation information infrastructure on a regional or local scale has potential for widespread economic and national security effects.
- Marketplace pressures and increasing utilization of IT make large-scale, multimodal disruptions more likely in the future. As the infrastructure becomes more interconnected and interdependent, the transportation industry will increasingly rely on information technology to perform its most basic business functions. As this occurs, it becomes more likely that information system failures could result in large-scale disruptions of multiple modes of the transportation infrastructure.
- There is a need for a broad-based infrastructure assurance awareness program to assist all modes of transportation.
- The transportation industry could leverage ongoing research and development initiatives to improve the security of the transportation information infrastructure.

***Electronics vulnerable to EMP permeate the transportation infrastructures.***

<sup>17</sup> NSTAC Information Infrastructure Group Report, June 1999, <<http://www.ncs.gov/NSTAC/NSTACXXII/Reports/NSTAC22-IIIG.pdf>>.

- There is a need for closer coordination between the transportation industry and other critical infrastructures.

The imperative to achieve superior performance has also led to a tremendous increase in the use of electronics that are potentially vulnerable to EMP. The internal combustion engine provides a familiar example of this phenomenon. Modern engines utilize electronics to increase performance, increase fuel efficiency, reduce emissions, increase diagnostic capability, and increase safety.

To gauge the degree of vulnerability of transportation infrastructures to EMP, the Commission has conducted an assessment of selected components of these infrastructures that are necessary to their operations. The assessment relied on testing where feasible, surveys and analyses for equipment and facilities for which testing was impractical, and reference to similarities to equipment for which EMP vulnerability data exists.

Based on this assessment, significant degradation of the transportation infrastructures are likely to occur in the immediate aftermath of an EMP attack. For example, municipal road traffic will likely be severely congested, possibly to the point of wide-area gridlock, as a result of traffic light malfunctions and the fraction of operating cars and trucks that will experience both temporary and in some cases unrecoverable engine shutdown. Railroad traffic will stop if communications with railroad control centers are lost or railway signals malfunction. Commercial air traffic will likely cease operations for safety and other traffic control reasons. Ports will stop loading and unloading ships until commercial power and cargo hauling infrastructures are restored.

The ability of the major transportation infrastructure components to recover depends on the plans in place and the availability of resources—including spare parts and support from other critical infrastructures upon which transportation is dependent. Transportation infrastructures have emergency response procedures in place; however, they do not explicitly address conditions that may exist for an EMP attack, such as little or no warning time and simultaneous disruptions over wide areas. Restoration times will depend on the planning and training carried out, and on the availability of services from other infrastructures—notably power, fuel, and telecommunications.

## STRATEGY FOR PROTECTION AND RECOVERY

### *RAILROADS*

Railroad operations are designed to continue under stressed conditions. Backup power and provisioning is provided for operations to continue for days or even weeks at reduced capacity. However, some existing emergency procedures, such as transferring

operations to backup sites, rely on significant warning time, such as may be received in a weather forecast before a hurricane. An EMP attack may occur without warning, thereby compromising the viability of available emergency procedures. Therefore, under the overall leadership of the DHS, the government and private sectors should work together to implement the general approach described in Strategy and Recommendations, page 11.

Specific actions should include:

- Heighten railroad officials' awareness of the possibility of EMP attack without warning that would produce wide-area, long-term disruption and damage to electronic systems.
- Perform test-based EMP assessments of railroad traffic control centers and retrofit modest EMP protection into these facilities, thereby minimizing the potential for adverse long term EMP effects. The emphasis of this effort should be on electronic control and telecommunication systems.

#### *TRUCKING AND AUTOMOBILES*

Emphasizing prevention and emergency clearing of traffic congestion in this area, DHS should coordinate a government and private sector program to:

- Initiate an outreach program to educate State and local authorities and traffic engineers on EMP effects and the expectation of traffic signal malfunctions, vehicle disruption and damage, and consequent traffic congestion.
- Work with municipalities to formulate recovery plans, including emergency clearing of traffic congestion and provisioning spare controller cards that could be used to repair controller boxes.
- Sponsor development of economical protection modules—preliminary results for which are already available from Commission-sponsored research—that could be retrofitted into existing traffic signal controller boxes and installed in new controller boxes during manufacture.
- Sponsor development of automobile robustness specifications and testing for EMP. These specifications should be implemented by augmenting existing specifications for gaining immunity to transient electromagnetic interference (EMI), rather than by developing separate specifications for EMP.

#### *MARITIME SHIPPING*

The essential port operations to be safeguarded are ship traffic control, cargo loading and unloading, and cargo storage and movement (incoming and outgoing). Ship traffic control is provided by the Coast Guard, which has robust backup procedures in

place. Cargo storage and movement are covered by other transportation infrastructure recommendations. Therefore, focusing on cargo operations in this area, DHS should coordinate a government and private sector program to:

- Heighten port officials' awareness of the wide geographic coverage of EMP fields, the risk due to loss of commercial power for protracted time-intervals, and the need to evaluate the practicality of providing emergency generators for at least some portion of port and cargo operations.
- Assess the vulnerability of electric-powered loading/unloading equipment. Review the electromagnetic protection already in place for lightning, and require augmentation of this protection to provide significant EMP robustness.
- Coordinate findings with the "real-time" repair crews to ensure they are aware of the potential for EMP damage. Based on the assessment results, recommend spares provisions so that repairs can be made in a timely manner.
- Assess port data centers for the potential loss of data in electronic media. Provide useful measures of protection against EMP causing loss of function and/or data.
- Provide protected off-line spare parts and computers sufficient for minimum essential operations.
- Provide survivable radio and satellite communication capabilities for the Coast Guard and the Nation's ports.

#### *COMMERCIAL AVIATION*

In priority order, it must be ensured that airplanes caught in the air during an EMP attack can land safely, that critical recovery assets are protected, and that contingency plans for an extended no-fly period are developed. Thus, DHS should coordinate a government program in cooperation with the FAA to perform an operational assessment of the air traffic control system to identify a "thin-line" that provides the minimal essential capabilities necessary to return the air traffic control capability to at least a basic level of service after an EMP attack. Based on the results of this operational assessment, develop tactics for protection, operational workarounds, spares provisioning, and repairs to return to a minimum-essential service level.



## FOOD INFRASTRUCTURE

### NATURE OF THE PROBLEM

EMP can damage or disrupt the infrastructure that supplies food to the population of the United States. Recent federal efforts to better protect the food infrastructure from terrorist attack tend to focus on preventing small-scale disruption of the food infrastructure, such as would result from terrorists poisoning some food. Yet an EMP attack could potentially disrupt the food infrastructure over a large region encompassing many cities for a protracted period of weeks to months.

Technology has made possible a dramatic revolution in US agricultural productivity. The transformation of the United States from a nation of farmers to a nation where less than 2 percent of the population is able to feed the other 98 percent and supply export markets is made possible only by technological advancements that, since 1900, have increased the productivity of the modern farmer by more than 50-fold. Technology, in the form of knowledge, machines, modern fertilizers and pesticides, high-yield crops and feeds, is the key to this revolution in food production. Much of the technology for food production directly or indirectly depends upon electricity, transportation, and other infrastructures.

The distribution system is a chokepoint in the US food infrastructure. Supermarkets typically carry only enough food to provision the local population for 1 to 3 days. Supermarkets replenish their stocks on virtually a daily basis from regional warehouses that usually carry enough food to supply a multi-county area for about one month. The large quantities of food kept in regional warehouses will do little to alleviate a crisis if it cannot be distributed to the population in a timely manner. Distribution depends largely on a functioning transportation system.

### MITIGATION AND RESPONSIBILITY

Federal, state, and regional governments should establish plans for assuring that food is available to the general population in case of major disruption of the food infrastructure. Planning to locate, preserve, deliver, distribute, and ration existing stockpiles of processed and unprocessed food, including food stockpiled by the Department of Agriculture, Department of Defense, and other government agencies, will

be an important component of maintaining the food supply. Planning to protect, deliver, and ration food from regional warehouses, under conditions where an EMP attack has disrupted the power, transportation, and other infrastructures for a protracted period, should be a priority. Plans to process and deliver private and government grain stockpiles would significantly supplement the processed food stored in regional warehouses. According to the USDA's National Agricultural Statistical Service, total private grain stockpiles in the United States amount to over 255 million metric tons. Federal grain stockpiles held by the Commodity Credit Corporation exceed 1.7 million metric tons, with 1.6 million metric tons of that amount dedicated to the Bill Emerson Humanitarian Trust for Overseas Emergency. Planning should include an assessment of how much food the population of the United States would need in an emergency when the food infrastructure is disrupted for a protracted period. Food stockpiles should be increased if existing stockpiles of food appear to be inadequate.

Presidential initiatives have designated the Department of Homeland Security as the lead agency responsible for the security of the food infrastructure, overseeing and working with the Department of Agriculture. Currently, under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act), the President "is authorized and directed to assure that adequate stocks of food will be ready and conveniently available for emergency mass feeding or distribution" in the United States. The Stafford Act should be amended to provide for plans to locate, protect, and distribute existing private and government stockpiles of food, and to provide plans for distribution of existing food stockpiles to the general population in the event of a national emergency.

## WATER SUPPLY INFRASTRUCTURE

National-level responsibilities have already been assigned to the Department of Homeland Security (DHS) and the Environmental Protection Agency (EPA) to protect the water infrastructure from terrorist threats. A recent Presidential Directive establishes new national policy for protection of our Nation's critical infrastructures against terrorist threats that could cause catastrophic health effects.<sup>18</sup> EPA is the designated lead agency for protection of drinking water and water treatment systems. DHS and EPA should ensure that protection includes EMP attack among the recognized threats to the water infrastructure.

---

<sup>18</sup> Homeland Security Presidential Directive – 7, *Critical Infrastructure Identification, Prioritization, and Protection*. December 17, 2003.

## EMERGENCY SERVICES

### VULNERABILITIES

An EMP attack will result in diminished capabilities of emergency services during a time of greatly increased demand upon them. The EMP vulnerability of emergency services systems is primarily due to the susceptibility of computer and communications equipment, and secondarily due to likely commercial electric power outages. Recent test results indicate that some failures of computers and network equipment can be expected at low EMP field levels; at higher levels, much more pervasive equipment failures are expected. Mobile radio communications equipment can be expected to experience disruption and failure at EMP threat levels that are likely to be experienced. Moreover, emergency services are critically dependent on the commercial telephone network, on electric power, and thus on fuel for backup generators. Degradation in these capabilities following an EMP attack is likely, as discussed previously, thereby providing another source of cascading infrastructure failure.

### RECOMMENDED STRATEGY FOR PROTECTION AND RECOVERY

The Department of Homeland Security must develop a strategy for protection and recovery of emergency services that emphasizes the inclusion of the EMP threat in planning and training and the establishment of technical standards for EMP protection of critical equipment. The Department of Homeland Security, including its Federal Emergency Management Agency (FEMA), and state and local governments should augment existing plans and procedures to address both immediate and long-term emergency services response to EMP attack. Plans should include provision for early warning notification, and a protection/recovery protocol based on graceful degradation and rapid recovery that emphasizes a balance between limited hardening and provisioning of spare components, as well as training for their use in emergency reconstitution. In addition, the Department of Homeland Security should provide technical support, guidance, and assistance to state and local governments, as well as to other federal departments and agencies, to ensure the EMP survivability or rapid recovery of critical emergency services networks and equipment.

## SPACE SYSTEMS

Over the past few years, there has been increased focus on US space systems in low Earth orbits and their unique vulnerabilities, among which is their susceptibility to nuclear detonations at high altitudes—the same events that produce EMP. It is also important to include, for the protection of a satellite-based system in any orbit, its control system and ground infrastructure, including up-link and down-link facilities.

Commercial satellites support many significant services for the Federal government, including communications, remote sensing, weather forecasting, and imaging. The national security and homeland security communities use commercial satellites for critical activities, including direct and backup communications, emergency response services, and continuity of operations during emergencies. Satellite services are important for national security and emergency preparedness telecommunications because of their ubiquity and separation from other communications infrastructures.

The Commission to Assess United States National Security Space Management and Organization conducted an assessment of space activities that support US national security interests, and concluded that space systems are vulnerable to a range of attacks due to their political, economic, and military value.<sup>19</sup> Satellites in low Earth orbit generally are at very considerable risk of severe lifetime degradation or outright failure from collateral radiation effects arising from an EMP attack on ground targets.

The Department of Homeland Security and the Department of Defense should jointly execute a systematic assessment of the significance of each space system, particularly those in low Earth orbits, to missions such as the continuity of government, strategic military force protection, and the protection of critical tactical force support functions. Information from this assessment and associated cost and risk judgments will inform senior government decision making regarding protection and performance-assurance of these systems, so that missions can be executed with the required degrees of surety in the face of the possible threats.

---

<sup>19</sup> *Report of the Commission to Assess United States National Security Space Management and Organization*, January 11, 2001.

## GOVERNMENT

DHS should give priority to measures to ensure that the President and other senior Federal officials can exercise informed leadership of the Nation in the aftermath of an EMP attack, and to improving post-attack response capabilities at all levels of government.

The President, Secretary of Homeland Security, and other senior officials must be able to manage the national recovery in an informed and reliable manner. Current national capabilities were developed for Cold War scenarios in which it was imperative that the President have assured connectivity to strategic retaliatory forces. While this is still an important requirement, there is a new need for considerably broader, robust connectivity between national leaders, government at all levels, and key organizations within each infrastructure sector so that the status of infrastructures can be assessed in a reliable and comprehensive manner and their recovery and reconstitution intelligently managed. The Department of Homeland Security, working through the Homeland Security Council, should give high priority to identifying and achieving the minimum levels of robust connectivity needed for recovery following EMP attack. In doing this, DHS should give particular emphasis to exercises that evaluate the robustness of the solutions being implemented.

Working with state authorities and private-sector organizations, the Department of Homeland Security should develop draft protocols for implementation by emergency and other government responders following EMP attack, Red Team these extensively, and then institutionalize validated protocols through issuance of standards, training, and exercises.



## KEEPING THE CITIZENRY INFORMED

Support to National leadership also involves measures to ensure that the President can communicate effectively with the citizenry. Although the US can improve prevention, protection, and recovery in the face of an EMP attack to levels below those that would have catastrophic consequences for the Nation, an EMP attack would still cause substantial disruption, even under the best of circumstances. Many citizens would be without power, communications and other services for days—or perhaps substantially longer—before full recovery could occur. During that interval, it will be crucial to provide a reliable channel of information to those citizens to let them know what has happened, the current situation, when help of what types for them might be available, what their governments are doing, and the host of questions which, if not answered, are certain to create more instability and suffering for the affected individuals, communities, and the Nation as a whole.

## PROTECTION OF MILITARY FORCES

The end of the Cold War relaxed the discipline for achieving EMP survivability within the Department of Defense, and gave rise to the perception that an erosion of EMP survivability of military forces was an acceptable risk. EMP simulation and test facilities have been mothballed or dismantled, and research concerning EMP phenomena, hardening design, testing, and maintenance has been substantially decreased. However, the emerging threat environment, characterized by a wide spectrum of actors that include near-peers, established nuclear powers, rogue nations, sub-national groups, and terrorist organizations that either now have access to nuclear weapons and ballistic missiles or may have such access over the next 15 years have combined to place the risk of EMP attack and adverse consequences on the US to a level that is not acceptable.

Current policy is to continue to provide EMP protection to strategic forces and their controls; however, the end of the Cold War has relaxed the discipline for achieving and maintaining that capability within these forces. The Department of Defense must continue to pursue the strategy for strategic systems to ensure that weapons delivery systems of the New Triad are EMP survivable, and that there is, at a minimum, a survivable “thin-line” of command and control capability to detect threats and direct the delivery systems. The Department of Defense has the capability to do this, and the costs can be within reasonable and practical limits.

The situation for general-purpose forces (GPF) is more complex. The success of these forces depends on the application of a superior force at times and places of our choosing. We accomplish this by using a relatively small force with enormous technological advantages due to superior information flow, advanced warfighting capabilities, and well-orchestrated joint combat operations. Our increasing dependence on advanced electronics systems results in the potential for an increased EMP vulnerability of our technologically advanced forces, and if unaddressed makes EMP employment by an adversary an attractive asymmetric option.

The United States must not permit an EMP attack to defeat its capability to prevail. The Commission believes it is not practical to protect all of the tactical forces of the US and its coalition partners from EMP in a regional conflict. A strategy of replacement and reinforcement will be necessary. However, there is a set of critical capabilities that is essential to tactical regional conflicts that must be available to these

reinforcements. This set includes satellite navigation systems, satellite and airborne intelligence and targeting systems, an adequate communications infrastructure, and missile defense.

The current capability to field a tactical force for regional conflict is inadequate in light of this requirement. Even though it has been US policy to create EMP-hardened tactical systems, the strategy for achieving this has been to use the DoD acquisition process. This has provided many equipment components that meet criteria for durability in an EMP environment, but this does not result in confidence that fielded forces, as a system, can reliably withstand EMP attack. Adherence to the equipment acquisition policy also has been spotty, and the huge challenge of organizing and fielding an EMP-durable tactical force has been a disincentive to applying the rigor and discipline needed to do so.

EMP durability should be provided to a selected set of tactical systems such that it will be practical to field tactical forces that cannot be neutralized by an EMP attack. The Department of Defense must perform a capabilities-based assessment of the most significant EMP threats to its tactical capabilities and develop strategies for coping with these threats in a reliable and effective manner.

Overall, little can be accomplished without the sustained attention and support of the leadership of the Department of Defense and Congress. This will require the personal involvement and cooperation among the Secretary of Defense, the Chairman of the Joint Chiefs, the Service Chiefs, and the appropriate congressional oversight committees in creating the necessary climate of concern; overseeing the development of strategy; and reaffirming the criticality of survivable and endurable military forces, including command, control, and communications (C3) in updated policy guidance, implementation directives, and instructions. Congressionally mandated annual reports from the Secretary of Defense and the Chairman of the Joint Chiefs on the status and progress for achieving EMP survivability of our fighting forces will emphasize the importance of the issue and help ensure that the necessary attention and support of the DoD leadership continues.

## APPENDIX A

### THE COMMISSION AND ITS METHOD

The Commission used a capability-based methodology to estimate potential EMP threats over the next 15 years.<sup>1</sup> The objective was to identify the range of plausible adversary EMP attack capabilities that cannot be excluded by prudent decision makers responsible for national and homeland security.

Bases for this assessment included current intelligence estimates of present and near-term military capabilities; current and past engineering accomplishments (what are adversaries likely to be capable of achieving, given accomplishments in other programs at comparable stages of development?); and trends impacting adversary military capabilities through 2018. In line with its capabilities-based approach, the Commission did not attempt to establish the relative likelihood of EMP strikes versus other forms of attack.

*...a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered looks strange; what looks strange is therefore improbable; what seems improbable need not be considered seriously.*

—Thomas C. Schelling, Foreword, in Roberta Wohlstetter, Pearl Harbor: Warning and Decision, Stanford University Press, 1962, p. vii.

Intelligence community organizations and the National Nuclear Security Administration's nuclear weapon laboratories (Lawrence Livermore, Los Alamos, and Sandia) provided excellent technical support to the Commission's analyses.<sup>2</sup> The Institute for Defense Analyses hosted and developed technical analyses for the Commission. While it benefited from these inputs, the Commission developed an independent assessment. Views expressed in this report are solely attributable to the Commission.

The Russian Federation (RF) has a sophisticated understanding of EMP that derives in part from the test era when the Soviet Union did high-altitude atmospheric tests

<sup>1</sup> Rob Mahoney, Capabilities-Based Methodology for Assessing Potential Adversary Capabilities, March 2004.

<sup>2</sup> The Commission's report and associated documents provide the necessarily classified assessments of future adversary capabilities for EMP attack and weapon issues.

over its own territory, impacting civilian infrastructures. To benefit from Russian expertise, the Commission:

- Sponsored research projects at Russian scientific institutions.
- Hosted a September 2003 US/Russian symposium on EMP at which presentations were given by Russian general officers.
- Sponsored a December 2003 technical seminar on EMP attended by scientists from the Russian Federation and the United States.

The Commission also reviewed additional relevant foreign research and programs and assessed foreign perspectives on EMP attacks.

In considering EMP, the Commission also gave attention to the coincident nuclear effects that would result from a detonation that produces EMP, e.g., possible disruption of the operations of, or damage to, satellites in space.

Different types of nuclear weapons produce different EMP effects. The Commission limited its attention to the most strategically significant cases in which detonation of one or few nuclear warheads could result in widespread, potentially long-duration disruption or damage that places at risk the functioning of American society or the effectiveness of US military forces.

In addition to examining potential threats, the Commission was charged to assess US vulnerabilities (civilian and military) to EMP and to recommend measures to counter EMP threats. For these purposes, the Commission reviewed research and best practices within the United States and other countries. Early in this review it became apparent that only limited EMP vulnerability testing had been accomplished for modern electronic systems and components. To partially remedy this deficit, the Commission sponsored illustrative testing; results are presented in the Commission's report.

Commissioners brought to this task a wide range of expertise, including service as an advisor to the President; senior management experience in both civilian and military agencies, national laboratories, and the corporate sector; and technical expertise in the design of nuclear weapons and in the hardening of systems against nuclear weapon effects.

## APPENDIX B

### COMMISSIONERS

*Dr. William R. Graham* is Chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. He is also Chairman of the Board and Chief Executive Officer of National Security Research Inc. (NSR), a Washington-based company that conducts technical, operational, and policy research and analysis related to US national security. In the recent past he has served as a member of several high-level study groups, including the Department of Defense Transformation Study Group, the Commission to Assess United States National Security Space Management and Organization (the Rumsfeld Commission on Space), and the Commission to Assess the Ballistic Missile Threat to the United States (also led by Hon. Donald Rumsfeld). From 1986–89 Dr. Graham was the director of the White House Office of Science and Technology Policy while he served concurrently as Science Advisor to President Reagan, Chairman of the Federal Joint Telecommunications Resources Board, and member of the Arms Control Experts Group. For 11 years he served as a member of the Board of Directors of the Watkins-Johnson Company.

*Dr. John S. Foster, Jr.*, is Chairman of the Board of GKN Aerospace Transparency Systems, chairman of Technology Strategies and Alliances, and consultant to Northrop Grumman Corporation, Sikorsky Aircraft Corp., Ninesigma, and Defense Group. He retired from TRW as Vice President, Science and Technology, in 1988 and continued to serve on the Board of Directors of TRW from 1988 to 1994. Dr. Foster was Director of Defense Research and Engineering for the Department of Defense from 1965–1973, serving under both Democratic and Republican administrations. In other distinguished service, Dr. Foster has been on the Air Force Scientific Advisory Board, the Army Scientific Advisory Panel, and the Ballistic Missile Defense Advisory Committee, Advanced Research Projects Agency. Until 1965, he was a panel consultant to the President's Science Advisory Committee, and from 1973–1990 he was a member of the President's Foreign Intelligence Advisory Board. He is a member of the Defense Science Board, which he chaired from January 1990–June 1993. From 1952–1962, Dr. Foster was with Lawrence Livermore National Laboratory (LLL), where he began as a Division Leader in experimental physics, became Associate Director in 1958, and became Director of LLL and Associate Director of the Lawrence Berkeley National Laboratory in 1961.

*Mr. Earl Gjelde* is the Managing Director and Chief Executive Officer of Summit Group International, Ltd.; Summit Energy Group, Ltd.; Summit Energy International 2000, LLC; and Summit Power NW, LLC, primary participants in the development of over 5,000 megawatts of natural gas fired electric and wind generating plants within the United States. He has also held a number of government posts, serving as President George Herbert Walker Bush's Under (now called Deputy) Secretary and Chief Operating Officer of the US Department of the Interior (1989) and as President Ronald Reagan's Under Secretary and Chief Operating Officer of the US Department of the Interior (1985–1988). While in the Reagan administration he served concurrently as Special Envoy to China (1987), Deputy Chief of Mission for the US-Japan Science and Technology Treaty (1987–1988), and Counselor for Policy to the Director of the National Critical Materials Council (1986–1988); the Counselor to the Secretary and Chief Operating Officer of the US Department of Energy (1982-1985); and Deputy Administrator,



Chief Operating Officer, and Power Manager of the Bonneville Power Administration (1980-1982). Prior to 1980, he was a principal officer of the Bonneville Power Administration.

*Dr. Robert J. Hermann* is a senior partner of Global Technology Partners, LLC, a Boston-based investment firm that focuses on technology, defense aerospace, and related businesses worldwide. In 1998, Dr. Hermann retired from United Technologies Corporation, where he was Senior Vice President, Science and Technology. Prior to joining UTC in 1982, Dr. Hermann served 20 years with the National Security Agency with assignments in research and development, operations, and NATO. In 1977, he was appointed Principal Deputy Assistant Secretary of Defense for Communications, Command, Control, and Intelligence. In 1979, he was named Assistant Secretary of the Air Force for Research, Development, and Logistics and concurrently was Director of the National Reconnaissance Office.

*Mr. Henry (Hank) M. Kluepfel* is a Corporate Vice President for Corporate Development and Chief Scientist in the Enterprise Security Solutions Group of SAIC. He is the company's leading cyberspace security advisor to the President's National Security Telecommunications Advisory Committee (NSTAC) and the Network Reliability and Interoperability Council (NRIC). Mr. Kluepfel is widely recognized for his 30-plus years of experience in security technology research, design, tools, forensics, risk reduction, education, and awareness, and he is the author of industry's de facto standard security base guideline for the Signaling System Number 7 (SS7) networks connecting and controlling the world's public telecommunications networks. In past affiliations with Telcordia Technologies (formerly Bellcore), AT&T, BellSouth and Bell Labs, he led industry efforts to protect, detect, contain, and mitigate electronic and physical intrusions and led the industry's understanding of the need to balance technical, legal, and policy-based countermeasures to the then emerging hacker threat. He is recognized as a Certified Protection Professional by the American Society of Industrial Security and is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

*General (USAF, Ret.) Richard L. Lawson* is Chairman of Energy, Environment and Security Group, Ltd., and former President and CEO of the National Mining Association. He also serves as Vice Chairman of the Atlantic Council of the U.S; Chairman of the Energy Policy Committee of the US Energy Association; Chairman of the United States delegation to the World Mining Congress; and Chairman of the International Committee for Coal Research. Active duty positions included serving as Military Assistant to the President; Chief of Staff, Supreme Headquarters Allied Powers Europe; Director for Plans and Policy, Joint Chiefs of Staff; Deputy Director of Operations, Headquarters US Air Force; and Deputy Commander in Chief, US European Command.

*Dr. Gordon K. Soper* is Group Vice President of Defense Group Inc., responsible for broad direction of corporate goals relating to company support of government customers in areas of countering the proliferation of weapons of mass destruction, chemical/biological defense and domestic preparedness, treaty verification research, nuclear arms control and development of new business areas and growth of technical staff. He provides senior-level technical support on a range of task areas to the Defense Threat Reduction Agency (DTRA), the Chemical and Biological National Security Program of National Nuclear Security Administration, and the Counterproliferation and Chem/Bio Defense Office of the Office of the Secretary of Defense. Previously, Dr. Soper was Principal Deputy to the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Programs (ATSD (NCB); Director, Office of Strategic and Theater Nuclear Forces Command, Control and Communications (C3) of the Office of the

Assistant Secretary of Defense (C3I); and Associate Director for Engineering and Technology/Chief Scientist at the Defense Communications Agency.

*Dr. Lowell L. Wood, Jr.*, is a member of the Technical Advisory Group, US Senate Select Committee on Intelligence; a member of the Undersea Warfare Experts Group, US House of Representatives Committee on Armed Services; a visiting fellow at the Hoover Institution and Stanford University; and an officer and member of the Board of Directors of the Fannie and John Hertz Foundation. He is also a member of the Director's technical staff, University of California Lawrence Livermore National Laboratory, where he has held numerous positions since 1972.

*Dr. Joan Woodard* is Executive Vice President and Deputy Director of Sandia National Laboratories, responsible for all of Sandia's programs, operations, staff, and facilities. She is also responsible for the laboratory's strategic planning. Prior to her current appointment, Dr. Woodard was Vice President of the Energy, Information and Infrastructure Technology Division, where her responsibilities included energy-related projects in fossil energy, solar, wind, geothermal, geosciences, fusion, nuclear power safety and severe accident analysis, and medical isotope processing; environment-related programs in remediation, nuclear waste management and repository certification, and waste minimization; information technology programs in information surety, command and control systems, and distributed information systems; and programs responsible for security of the transportation of nuclear weapons and special nuclear materials, and safety of commercial aviation. Over 80% of the programs included industrial or academic partners, and the nature of the work ranged from basic research to prototype systems evaluation.



VOLUME I

# Assessing the Threat from Electromagnetic Pulse (EMP)

Executive Report

JULY 2017

Report of the Commission to Assess the Threat to the United States  
from Electromagnetic Pulse (EMP) Attack



# Assessing the Threat from Electromagnetic Pulse (EMP)

## Executive Report

**July 2017**

REPORT OF THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES  
FROM ELECTROMAGNETIC PULSE (EMP) ATTACK

---



The cover photo depicts Fishbowl Starfish Prime at 0 to 15 seconds from Maui Station in July 1962, courtesy of Los Alamos National Laboratory.

This report is a product of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. The Commission was established by Congress in the FY2001 National Defense Authorization Act, Title XIV, and was continued per the FY2016 National Defense Authorization Act, Section 1089.

The Commission completed its information-gathering in June 2017. The report was cleared for open publication by the DoD Office of Prepublication and Security Review on April 9, 2018.

This report is unclassified and cleared for public release.

TABLE OF CONTENTS

---

EXECUTIVE SUMMARY ..... 1

OBSERVATIONS, ANALYSIS, AND RECOMMENDATIONS ..... 4

    The EMP Threat ..... 4

    Barriers to Effective Protection from EMP ..... 6

    Late-Time EMP Fields and Effects (E3) ..... 13

    Testing Selected EMP-vulnerable Full-system Equipment to Failure..... 15

    Intelligence Community Assessment of the EMP Threat..... 16

CONCLUSIONS ..... 17

APPENDIX A   Legislation Re-establishing the Commission..... 19

APPENDIX B   High Altitude Nuclear Explosion-Generated Electromagnetic Effects..... 20

BIOGRAPHIES..... 22

    Commissioners..... 22

    Senior Advisors..... 24

COMMISSION REPORTS ..... 27

## ACRONYMS AND ABBREVIATIONS

---

DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
ELECTRA	Electromagnetic Effects Comparison Test and Reliability Assessment
EMP	electromagnetic pulse
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
FERC	Federal Energy Regulatory Commission
HEMP	high-altitude electromagnetic pulse
NERC	North American Electric Reliability Corporation
NRC	Nuclear Regulatory Commission

## PREFACE

---

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (herein and elsewhere referred to as “the EMP Commission”) was re-established by the National Defense Authorization Act (NDAA) for Fiscal Year 2016 on November 25, 2015, and funded by the appropriation for the Commission on December 18, 2015. Delays by the Department of Defense in providing funding, clearance support, and contractor support to the Commission throughout 2016 delayed the first meeting until January 2017. The Commission’s statutory mandate terminated at the end of June 2017 in accord with the terms of the NDAA. EMP is a complex subject, and the DoD provided only limited support beyond this time to allow the Commission to complete its work even though funding to continue was available. As a result, the Commission could not adequately complete the full scope of the Congressional charge as described in Appendix A. This report is therefore necessarily limited, yet the Commission is confident this material contained herein is accurate and trusts it is valuable to the recipients.

Following the last meeting of the EMP Commission on June 8-9, 2017, global events have strengthened public awareness of the worldwide vulnerability of critical infrastructures to high altitude EMP. North Korean state news, KCNA, displayed photos of an alleged thermonuclear weapon and claimed on September 3, 2017, “The H-bomb, the explosive power of which is adjustable from tens of kilotons to hundreds of kilotons, is a multi-functional thermonuclear nuke [sic] with great destructive power which can be detonated even at high altitudes for super-powerful EMP (electromagnetic pulse) attack according to strategic goals.” The United States, its territories, and allies are therefore the target of current threats by the government of North Korea that specifically include EMP, and also include further development and exploitation of high altitude EMP weapons.

## EXECUTIVE SUMMARY

---

The critical national infrastructure in the United States faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, as well as from natural EMP from a solar superstorm. During the Cold War, the U.S. was primarily concerned about an EMP attack generated by a high-altitude nuclear weapon as a tactic by which the Soviet Union could suppress the U.S. national command authority and the ability to respond to a nuclear attack—and thus negate the deterrence value of assured nuclear retaliation. Within the last decade, newly-armed adversaries, including North Korea, have been developing the ability and threatening to carry out an EMP attack against the United States. Such an attack would give countries that have only a small number of nuclear weapons the ability to cause widespread, long-lasting damage to critical national infrastructures, to the United States itself as a viable country, and to the survival of a majority of its population.

Major efforts have been undertaken by the Department of Defense to assure that the U.S. national command authority and U.S. strategic forces could survive and operate after an EMP attack. However, no major efforts were thought necessary to protect critical national infrastructures, relying on nuclear deterrence to protect them. With the development of small nuclear arsenals and long-range missiles by small, hostile, and potentially irrational adversaries, including North Korea, the threat of a nuclear EMP attack against the U.S. becomes one of the few ways that such a country could inflict devastating damage to the United States. It is critical, therefore, that the U.S. national leadership address the EMP threat as a critical and existential issue, and give a high priority to assuring the leadership is engaged and the necessary steps are taken to protect the country from EMP. Otherwise, foreign adversaries may reasonably consider such an attack as one which can gravely damage the U.S. by striking at its technological Achilles' heel without having to engage the U.S. military.

Protecting and defending the national electric grid and other critical infrastructures from cyber and EMP could be accomplished at reasonable cost and minimal disruption to the present systems that comprise U.S. critical infrastructure. This is commensurate with Trump Administration plans to repair and improve U.S. infrastructures, increase their reliability, and strengthen homeland defense and military capability. Continued failure to address the U.S. vulnerability to EMP generated by a high-altitude nuclear weapon invites such an attack.

The single most important action *that requires immediate action* to advance U.S. security and survivability is that the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat (*Recommendation 1*). Current institutional authorities and responsibilities—government, industry, regulatory agencies—are fragmented, incomplete,

under-resourced, and unable to protect and defend against foreign hostile EMP threats or solar superstorms.

The Commission highly commends President Trump's Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, signed on May 11, 2017. **The Commission strongly recommends that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection** (*Recommendation 2*), because all-out cyber warfare may well include nuclear EMP attack. Protecting against nuclear EMP will also protect against natural EMP from solar storms, although the converse is not true. The United States must take steps to mitigate its current state of vulnerability to these well-known natural and adversary EMP threats. To further this endeavor, **the Commission encourages the President to work with Congressional leaders to establish a joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership to achieve, on an accelerated basis, the protection of critical national infrastructures.** (*Recommendation 3*).

Across the U.S. government, the DoD and its supporting laboratories and contractors have by far the most knowledge, data, and experience related to the production of and survival from nuclear weapon-generated EMP. However, the DoD has largely failed to make this knowledge available to other government agencies and to the organizations that develop, build, and operate U.S. critical national infrastructure. For example, there has been a continuing unwillingness of the DoD to provide specific information about the EMP environment to the commercial community owing to classification restrictions. Today the DHS looks to the DOE to provide guidance and direction for protecting the national electric power grids. Such a course of action would take longer and cost more compared to establishing a program of cooperation with the knowledgeable parts of the DoD.

In the absence of an unclassified, well-informed U.S. late-time (E3) EMP threat specification [described in Appendix B], electric utilities, electrical equipment manufacturers, and electric research institutes have articulated their inability to design appropriate countermeasures and to justify cost recovery for capital investments programs. Accordingly, this Commission has prioritized the development of late-time E3 threat specifications, derived from openly available test data. As part of this assessment, Commission staff analyzed E3 EMP measurements from two nuclear high-altitude tests performed by the Soviet Union in 1962. Physicists with extensive experience in EMP modeling used these data waveforms and an understanding of the scaling relationships for the nuclear explosion-induced upper atmospheric heave phenomenon that produces the E3 EMP electromagnetic fields by disturbing the natural magnetic field of the Earth. Based on this analysis, **the Commission recommends that government agencies and industries adopt new standards to protect critical national infrastructures from damaging E3 EMP heave fields, with more realistic standards of 85 V/km** (*Recommendation 4*). Typical waveforms for commercial applications are included in Appendix B that should prove useful for the protection of the national power grids. **The Commission also recommends**



**electric grid equipment with long-replacement times such as large power transformers be tested to system failure** (*Recommendation 5*).

In the area of national intelligence, the Commission found that the classified report by the Joint Atomic Energy Intelligence Committee (JAEIC) on EMP issued in 2014 is factually erroneous and analytically unsound. **The Commission recommends the Director of National Intelligence circulate to all recipients of the 2014 JAEIC report the EMP Commission critique of that report and direct a new assessment be prepared that supersedes the 2014 JAEIC EMP report** (*Recommendation 6*). The new report should be reviewed by experts in the subject areas being addressed and circulated to all the recipients of the 2014 assessment.

## OBSERVATIONS, ANALYSIS, AND RECOMMENDATIONS

---

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack was previously convened by the Congress from 2001-2005 and from 2007-2008, and currently from 2016-2017.<sup>1,2</sup>

The current Commission assessment is consistent with the previous recommendations. In summary, the Commission sees the high-altitude nuclear explosion-generated electromagnetic pulse as an existential threat to the survival of the United States and its allies that can be exploited by major nuclear powers and small-scale nuclear weapon powers, including North Korea and non-state actors, such as nuclear-armed terrorists.

### THE EMP THREAT

The United States—and modern civilization more generally—faces a present and continuing existential threat from naturally occurring and manmade electromagnetic pulse assault and related attacks on military and critical national infrastructures. A nationwide blackout of the electric power grid and grid-dependent critical infrastructures—communications, transportation, sanitation, food and water supply—could plausibly last a year or longer.<sup>3</sup> Many of the systems designed to provide renewable, stand-alone power in case of an emergency, such as generators, uninterruptable power supplies (UPS), and renewable energy grid components, are also vulnerable to EMP attack.<sup>4</sup>

A long-term outage owing to EMP could disable most critical supply chains, leaving the U.S. population living in conditions similar to centuries past, prior to the advent of electric power.<sup>5</sup> In the 1800s, the U.S. population was less than 60 million, and those people had many skills and assets necessary for survival without today's infrastructure. An extended blackout today could result in the death of a large fraction of the American people through the effects of societal collapse, disease, and starvation. While national planning and preparation for such events could help mitigate the damage, few such actions are currently underway or even being contemplated.

---

<sup>1</sup> The EMP Commission has previously published two unclassified reports: *Executive Report* dated 2004, and *Critical National Infrastructures*, dated 2008.

<sup>2</sup> See Appendix A, "Legislation Re-establishing the Commission," National Defense Authorization Act for Fiscal Year 2016, Sec. 1089.

<sup>3</sup> For example, see E. Conrad, G. Gurtman, G. Kweder, M. Mandell, and W. White. *Collateral Damage to Satellites from an EMP Attack*, Report to the EMP Commission, DTRA-IR-10.22.

<sup>4</sup> Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *HEMP Direct Drive Testing of Sample Solar Systems. Report of the EMP Commission*. July 2017.

<sup>5</sup> National Security Telecommunications Advisory Committee (NSTAC). *People and Processes: Current State of Telecommunications and Electric Power*, January 31, 2006.

Combined-arms cyber warfare, as described in the military doctrines of Russia, China, North Korea, and Iran, may use combinations of cyber-, sabotage-, and ultimately nuclear EMP-attack to impair the United States quickly and decisively by blacking-out large portions of its electric grid and other critical infrastructures.<sup>6</sup> Foreign adversaries may aptly consider nuclear EMP attack a weapon that can gravely damage the U.S. by striking at its technological Achilles Heel, without having to confront the U.S. military. The synergism of such combined arms is described in the military doctrines of all these potential adversaries as the greatest revolution in military affairs in history—one which projects rendering obsolete many, if not all, traditional instruments of military power.

Any of several threats, as described here, must be considered:

- Solar superstorms can generate natural EMP over remarkably wide areas. Recurrence of the Carrington Event of 1859 is considered by many to be inevitable.<sup>7</sup> NASA estimates the likelihood of such an event to be 10 to 12 percent per decade, making it very likely that Earth will be affected by a solar superstorm within a matter of decades.<sup>8</sup> Such an event could blackout electric grids and other life-sustaining critical infrastructures, putting at risk the lives of many millions.
- Nuclear EMP attack might be conducted with only a single nuclear weapon detonated at high altitude or a few weapons at several hundred kilometers. These could be delivered by satellite, by a wide variety of long- and short-range missiles, including cruise and anti-ship missiles, by a jet doing a zoom-climb, or even by a high-altitude balloon. Some modes of attack could be executed relatively anonymously, thereby impairing deterrence.
- Russia, China, and North Korea now have the capability to conduct a nuclear EMP attack against the U.S. All have practiced or described contingency plans to do so.<sup>9</sup> Terrorists or other less-sophisticated actors also might mount a nuclear EMP attack if

---

<sup>6</sup> For example, see Army of the Islamic Republic of Iran, *Passive Defense: Approach to the Threat Center* (Tehran: Martyr Lt. General Sayad Shirazi Center for Education and Research, Spring 2010); Shen Weiguang, *World War, the Third World War—Total Information Warfare*; General Vladimir Slipchenko, *Non-Contact Wars* (Moscow: January 1, 2000) translated in FBIS CEP20001213000001; and comments on North Korean state news on 3 September 2017.

<sup>7</sup> R.A. Lovett. "What if the biggest solar storm on record happened today?" *National Geographic News*, March 4, 2011.

<sup>8</sup> P. Riley and J.J. Love, "Extreme geomagnetic storms: Probabilistic forecasts and their uncertainties," *Space Weather*, v. 15, Jan. 2017, pp. 53-64. The probability of an extreme geomagnetic storm on the scale of the Carrington event varies based on the type of distribution used in the analysis from 3 (lognormal) to 10 (power law) per decade; see also P. Riley, "On the probability of occurrence of extreme space weather," *Space Weather*, v. 10, Feb. 2012, pp. 2101-2114, which estimates 12 percent per decade.

<sup>9</sup> For example, see Army of the Islamic Republic of Iran, *Passive Defense: Approach to the Threat Center* (Tehran: Martyr Lt. General Sayad Shirazi Center for Education and Research, Spring 2010); Shen Weiguang, *World War, the Third World War—Total Information Warfare*; General Vladimir Slipchenko, *Non-Contact Wars* (Moscow: January 1, 2000) translated in FBIS CEP20001213000001; and comments on North Korean state news on 3 September 2017.

they have access to a suitable nuclear explosive. For missile delivery, no re-entry system or accurate missile guidance would be necessary.

- Cyber-attack, using computer viruses and related means, might be able to blackout much of the national electric grid for extended intervals. According to U.S. Cyber Command, Russia and China currently have such capability and it may only be a matter of time before other adversaries also gain a similar capability.<sup>10</sup>
- The U.S. electrical grid could be sabotaged by damaging extra-high-voltage (EHV) transformers using rifles, explosives, or non-nuclear EMP or directed energy weapons. Attacking less than a dozen key substations could result in protracted and widespread blackouts, according to the public statements of a past Chairman of the U.S. Federal Energy Regulatory Commission (FERC).<sup>11</sup> At least one substantive rehearsal of such an attack may have already taken place, at the Metcalf substation in the San Francisco Bay area.<sup>12</sup>
- The Commission highly commends President Trump's Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" signed on May 11, 2017. Including the potential for EMP as part of a cyber-attack is prudent when the current vulnerability of the U.S. electrical grid and critical infrastructures is taken into account.

***Recommendation 2:** The Commission strongly recommends that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection.*

## BARRIERS TO EFFECTIVE PROTECTION FROM EMP

The government's response to the EMP Commission recommendations made in 2008 is not encouraging.

In a 2011 study, the DoD's JASON advisory panel concluded that the federal response to the EMP risk "is poorly organized; no one is in charge, resulting in duplications and omissions between agencies."<sup>13</sup>

---

<sup>10</sup> Admiral Michael Rogers, Director, National Security Agency and Commander, U.S. Cyber Command. "Cybersecurity Threats: The Way Forward," Testimony, House Permanent Select Committee on Intelligence, Nov. 20, 2014.

<sup>11</sup> R. Smith. "U.S. Risks National Blackout From Small-Scale Attack," Wall Street Journal, March 12, 2014; and R. Smith. "How America Could Go Dark," Wall Street Journal, July 14, 2016.

<sup>12</sup> R. Smith. "Assault On California Power Station Raises Alarm On Potential For Terrorism," Wall Street Journal, February 5, 2014.

<sup>13</sup> MITRE, 2011. Impacts of Severe Space Weather on the Electric Grid, MITRE, 2011, Report JSR-11-320.

A survey of recent government reports that address the protection of critical infrastructure reveals that none mention EMP, although critical infrastructure risks, resilience, protection, and availability are central to each report and to each Departments' mission.<sup>14</sup>

During a hearing before the Senate Homeland Security and Government Affairs (SHSGA) Committee on July 22, 2015, the U.S. Government Accountability Office (GAO) acknowledged that none of the recommendations of the EMP Commission to protect the national grid from EMP have been implemented by DHS, DOE, U.S. FERC or the North American Electric Reliability Corporation (NERC).<sup>15</sup> The GAO report explained lack of progress in protecting the national electric grid from EMP as due to a lack of leadership, because no one was in charge of solving the EMP problem, as follows: "DHS and DOE, in conjunction with industry, have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks."<sup>16</sup>

In March 2016, GAO reported that none of the essential measures recommended by the EMP Commission to protect the national electric grid had been addressed by Federal agencies, as shown in Table 1. The report stated that agencies had primarily drafted industry standards and federal guidelines and have only completed related research reports rather than implementing the resulting recommendations.<sup>17</sup>

**Table 1: Status of Previous Recommendations from the EMP Commission**

<i>Recommendation</i>	<i>Action</i>
Expand and extend emergency power supplies	None
Extend black start capability	None
Prioritize and protect critical nodes	None
Expand and assure intelligent islanding capability	None
Assure protection of high-value generation assets	None
Assure protection of high-value transmission assets	None
Assure sufficient numbers of adequately trained recovery personnel	None

Some efforts have been made, but these have been frustrated by a lack of leadership. For example, in October 2016, President Obama issued a comprehensive Executive Order for

<sup>14</sup> These reports include *Mitigation of Power Outage Risks for Department of Defense Facilities and Activities 2015*, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (DHS), and *U.S. Department of Energy Strategic Plan 2014-2018*.

<sup>15</sup> The Nuclear Regulatory Commission could be added to the list of deficient government agencies in that it has failed to similarly protect the nuclear power reactors and spent fuel storage facilities for which they are responsible.

<sup>16</sup> U.S. Senate Committee on Homeland Security and Governmental Affairs. Full committee hearing on "Protecting the Electric Grid from the Potential Threats of Solar Storms and Electromagnetic Pulse," held July 22, 2015.

<sup>17</sup> Government Accountability Office. *Critical Infrastructure Protection: Federal Agencies Have Taken Actions To Address Electromagnetic Risks, But Opportunities Exist To Further Assess Risks And Strengthen Collaboration*, GAO-16-243, March 2016.

coordinating efforts to prepare the nation for space weather events.<sup>18</sup> The primary federal mechanism for coordination is the interagency Space Weather Operations, Research, and Mitigation (SWORM) task force. This Executive Order gave DHS overall leadership in geomagnetic disturbance preparedness and the DOE leadership in addressing grid impacts, yet neither department has yet done a credible job of preparing the U.S. for such storms. This minimal effort did not address preparing the nation for similar wide-area effects on the electric power grid caused by an EMP attack.

Despite advocacy for a combined standard to protect the U.S. bulk power system from both man-made EMP and natural occurring solar storms, FERC in May 2013 ordered development of operating procedures and hardware protection standards only for solar geomagnetic disturbances.<sup>19</sup> Upon recommendations of the designated Electric Reliability Organization, NERC, FERC issued guidance for operational procedures to cope with solar storms in FERC Order 779.<sup>20</sup> These procedures excluded owner-operator requirements to protect generating facilities with generator step-up transformers, even those that have experienced transformer fires and explosions in prior solar storms. After development of a benchmark model by a NERC Geomagnetic Disturbance Task Force, in September 2016 FERC issued a standard for phased assessments of potential hardware protections that utilities would perform over a period of years, but without any mandatory hardware-protection installations actually required.<sup>21</sup>

These scattered, incoherent, and inadequate responses are a clear indication that for at least the last decade, critical national infrastructure protection from EMP has been largely ignored or dismissed by major departments of the U.S. government. The unaddressed vulnerability of the U.S. to EMP is an incentive for hostile powers to attack or, at a minimum, to develop capabilities for HEMP attack.

### *Interagency Cooperation and Centralized Governance*

The DoD has, since 1962, understood the data, phenomena, magnitude, and importance of high-altitude electromagnetic pulse (HEMP) effects, and has applied that knowledge to certain military systems.<sup>22</sup> However, DoD has not adequately transferred that knowledge to other agencies of the government and to organizations that provide critical national infrastructures, such as electrical power and communications utilities. This is surprising because

---

<sup>18</sup> The White House. "Coordinating Efforts to Prepare the Nation for Space Weather Events," Executive Order 13744, October 13, 2016.

<sup>19</sup> FERC Order No. 779, Reliability Standards for Geomagnetic Disturbances, May 16, 2013.

<sup>20</sup> FERC Order No. 797, Reliability Standard for Geomagnetic Disturbance Operations, June 19, 2014.

<sup>21</sup> FERC Order No. 830, Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events, September 22, 2016. On the last full day of the Obama Administration, FERC denied four appeals for rehearing of Order 830, in FERC Order No. 830-A, January 19, 2017.

<sup>22</sup> Operation Fishbowl in 1962 was the last high-altitude nuclear test series conducted by the U.S. military.



the DoD depends upon these same critical national infrastructures for domestic military operations as well as the security of the nation. To the contrary, the DoD has withheld public distribution of and has classified much of the data and technology that underlies protection against EMP even though potential adversaries of the U.S. are generally familiar with such technology. It is interesting to note that some of the most useful data available for predicting the electromagnetic fields produced by a nuclear explosion have been derived from data published by the former Soviet Union.<sup>23</sup>

In the absence of technology transfer and other support by the DoD to other agencies of the government and the industries supporting critical national infrastructures, the DHS depends upon the DOE, as their Sector-Specific Agency, to provide guidance and direction for protecting the national electric power grids.<sup>24</sup> The DOE relies on the National Laboratories under its sponsorship to provide such guidance and direction. While it is possible to conduct new testing and analysis required to generate the data, such a course of action would take longer and cost more compared to establishing a program of cooperation with the knowledgeable offices and laboratories in the DoD. A more efficient alternative is establishing a DoD policy that makes much of the defense-controlled data concerning EMP technology available to the government agencies and industry that support the U.S. critical national electric power infrastructure.

### *Regulatory Conflicts of Interest*

The current institutional arrangements for protecting and improving the reliability of the electric grids and other critical infrastructures through the FERC and the NERC are not designed to address major national security threats to the electric power grids and other national critical infrastructures. Using FERC and NERC to achieve this level of national security has proven to be ineffectual. New institutional arrangements are needed to advance preparedness to guard against EMP and related threats to our critical national infrastructures.

The current U.S. power industry is largely self-regulated under FERC, NERC, Nuclear Regulatory Commission (NRC), and the electric power industry companies. The EMP Commission assesses that the existing regulatory framework for safeguarding the security and reliability of the electric power grid, which is based upon a partnership between the U.S. Government's FERC and the private non-profit NERC representing the utilities, is not set up to protect the U.S. against hostile EMP attack. For example, the standards for protecting the power grids from geomagnetic disturbances caused by solar storms prescribe threat levels

---

<sup>23</sup> One of the best references for understanding and protecting against EMP is a translation of a Soviet handbook, entitled, "The Physics of Nuclear Explosions," Ministry of Defense of the Russian Federation, Central Institute of Physics and Technology, Volumes 1 and 2, ISBN 5-02-015124-6, 1997.

<sup>24</sup> See the DHS Energy Sector overview at <https://www.dhs.gov/energy-sector>

below those recorded during major storms of historical record.<sup>25</sup> In May 2013, FERC ordered entities in the bulk power system to develop reliability standards to protect against solar geomagnetic disturbances (GMD). Generator operators were excluded. Despite multiple requests for FERC to develop a joint reliability standard for grid protection from both EMP and GMD hazards, NERC has only proposed limited standards for solar storm protection.<sup>26,27</sup> This can be attributed to the industry's desire to minimize protection requirements.

In public testimony before Congress, FERC has stated that it lacks regulatory power to compel NERC and the electric power industry to protect the grid from natural and nuclear EMP and other threats.<sup>28</sup> Consider the contrast in regulatory authority of the U.S. Federal Energy Regulatory Commission and similar regulatory agencies in the U.S. Government:

- The NRC has regulatory power to compel the nuclear power industry to incorporate nuclear reactor design features to make nuclear power safe. (To date, however, the NRC has not incorporated EMP survival criteria into design regulations. Further, that Commission has not required that spare transformers or emergency diesel generators be certified to be EMP-protected.)
- The U.S. Federal Aviation Administration (FAA) has regulatory power to compel the airline industry to ground aircraft considered unsafe, to change aircraft operating procedures considered unsafe, and to make repairs or improvements to aircraft in order to protect the lives of airline passengers.
- The U.S. Department of Transportation (DOT) has regulatory power to compel the automobile industry to install on cars safety glass, seatbelts, and airbags in order to protect the lives of the driving public.
- The U.S. Food and Drug Administration (FDA) has power to regulate the quality of food and drugs, and can ban under criminal penalty the sale of products deemed by the FDA to be unsafe to the public.
- The U.S. Environmental Protection Agency (EPA) has power to regulate clean air, clean water, and hazardous materials deemed by the EPA to be unsafe to the public.

---

<sup>25</sup> J.G. Kappenman and W. Radasky, *Examination of NERC GMD Standards and Validation of Ground Models and Geo-Electric Fields, Report to the EMP Commission*, July 28, 2017. See also Foundation for Resilient Societies, Comments Submitted on Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events, FERC Docket No. RM15-11-000, July 27, 2015; supplementary comments submitted August 10, 2015.

<sup>26</sup> Requests for rehearing of Order No. 830 were filed by the Foundation for Resilient Societies, Edison Electric Institute, Center for Security Policy, and Jewish Institute for National Security Affairs. These were denied in Docket No. RM15-11-001, issued January 19, 2017.

<sup>27</sup> U.S. Federal Energy Regulatory Commission. "Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events," Docket No. RM15-11-000; Order No. 830, issued January 21, 2016.

<sup>28</sup> Testimony of Joseph McClelland, U.S. FERC's Director of the Office of Electric Reliability, before the Senate Committee on Energy and Natural Resources (July 17, 2012); T. Sanders, "FERC's McClelland Calls For Enhanced Authority On Cyber-Security" Washington Energy Report, July 20, 2012.

Unlike the NRC, FAA, DOT, FDA, EPA, and most other U.S. government regulatory agencies, FERC does not have legal authority to compel the industry it is charged to regulate to act in the public interest. The U.S. FERC even lacks legal power to direct the electric utilities to install devices to protect the grid.

Currently, U.S. FERC only has the power to require NERC to propose a standard to protect the grid. NERC Standards are approved, or rejected, or remanded for further consideration by its membership, which is largely made up of representatives from the electric power industry. Once NERC proposes a standard to FERC, FERC cannot modify the standard, but must either accept or reject the proposed standard. If FERC rejects the proposed standard, NERC goes back to the drawing board, and the process starts all over again, often resulting in long delays for implementation of standards.

The DOE Quadrennial Energy Review released in January 2017 recommended, "... in the area of cybersecurity, Congress should provide FERC with authority to modify NERC-proposed reliability standards—or to promulgate new standards directly—if it finds that expeditious action is needed to protect national security in the face of fast-developing new threats to the grid. This narrow expansion of FERC's authority would complement DOE's national security authorities related to grid-security emergencies affecting critical electric infrastructure and defense-critical electricity infrastructure..."<sup>29</sup>

It is notable that this proposal would limit additional FERC authority to strengthen a reliability standard or to promulgate a new standard "in the area of cybersecurity." Although EMP hazards were not explicitly included in the proposed supplemental FERC authorities, EMP could be included under the cyber threat rubric as it directly debilitates cyber electronic systems.

Moreover, testifying before a House Energy and Commerce Subcommittee on February 1, 2017, the Chief Executive Officer of NERC expressed opposition to any Congressional grant of new FERC legislative authority to strengthen or directly promulgate any new grid reliability standard that NERC had not already proposed, thereby undermining the FERC's ability to protect the U.S. electric power grids from EMP attack.<sup>30</sup>

The geomagnetic disturbance standards proposed by the NERC, which the FERC has adopted to date, substantially underestimate the magnitude of historical and future geomagnetic disturbances. No standards for protecting the grid against nuclear or non-nuclear EMP weapons have been proposed or adopted.<sup>31</sup>

---

<sup>29</sup> U.S. Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the QER*, January 2017, pp. S-16 and 7-7.

<sup>30</sup> G.W. Cauley, *Hearing on the Electricity Sector's Efforts to Respond to Cybersecurity Threats*, Testimony before the House Subcommittee on Energy, Energy and Commerce Committee, February 1, 2017.

<sup>31</sup> Federal Energy Regulatory Commission (FERC) Order 779, *Final Rule on Reliability Standard for Geomagnetic Disturbances*, Reliability Standard EOP-010-1, June 25, 2014; FERC Order 830, *Transmission System Planned*

### *Recommendations to Improve Governance*

The Commission's chief recommendation is made to address the critical leadership deficiency.

***Recommendation 1:*** *The Commission recommends the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat.*

The 2017 Presidential initiative to repair and strengthen U.S. infrastructure, cyber security, homeland defense, and military capability presents a unique opportunity to include measures for EMP protection that could obviate the existential threats from solar superstorms and combined-arms cyber warfare.

A second recommendation in the area of governance is to ensure a whole-of-government approach to the challenge of EMP protection. A joint Presidential-Congressional Commission on critical infrastructure protection could engage the free world's preeminent experts on EMP and related threats to serve the interagency in a manner akin to other advisory Commissions. For example, between 1947 and 1974, the Atomic Energy Commission advised the administration on how to attain most quickly and most cost-effectively the protection essential to long-term national survival and well-being. Such a structure would help the U.S. move beyond the current state of vulnerability to well-understood natural and man-made EMP threats.

***Recommendation 3:*** *The Commission encourages the President to work with Congressional leaders to establish a joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership to achieve, on an accelerated basis, the protection of critical national infrastructures.*

Protecting the national electric grid and other critical infrastructures from the most severe of these threats—nuclear EMP attack—could be done in ways that protect against or significantly mitigate some other threats. Extensively tested, performance-proven technologies for EMP hardening have been developed and used by the DoD to protect critical military systems for over 50 years, and can be affordably adapted to protect electric grids and other critical infrastructures, at low-cost relative to that of an EMP catastrophe.

For example, the EMP Commission estimated in its 2008 report, critical parts of the national electric grid could be protected for about \$2 billion.

---

*Performance for Geomagnetic Disturbance Events, Reliability Standard TPL-007-1, Sep. 22, 2016, and FERC Order 830-A, Denying Rehearing (of Order 830), January 19, 2017.*

The U.S. knowledge base on EMP threat levels and waveforms is adequate. Likewise, EMP protection engineering is mature such that system protection programs can proceed immediately, without the need for lengthy additional research. The Commission is concerned that DOE and the Electric Power Research Institute (EPRI) are pursuing lengthy research and development programs to redefine environments and determine EMP system effects that introduce unnecessary delays in actual implementation of grid protection. The Commission finds that diverting these resources to pilot demonstration programs to protect selected sectors of the electric power grid would better serve the intent to protect the U.S. electrical grid. A strategic plan, along with the leadership to implement it, is needed now.

### LATE-TIME EMP FIELDS AND EFFECTS (E3)

Solar superstorms, more formally called coronal mass ejection events, produce fields similar to EMP E3 effects. A NASA analysis states that “historical aurora records suggest a return period of 50 years for Québec-level storms and 150 years for very extreme storms, such as the 1859 Carrington event.”<sup>32</sup> A high-altitude nuclear EMP event would also include higher frequency E1 and E2 fields. An understanding of the range of fields produced is required to understand their effects and the threat to the electrical grid.

To study the impact of these types of electromagnetic fields on extended electrical and communications transmission lines associated with the critical infrastructures, utilities need upper-bound, open-source information for the late-time (E3) high-altitude electromagnetic pulse threat waveform and its ground pattern. This need arises because of the effect of very low frequency electric field component (E3) coupled to horizontal electrical conductors, such as power transmission lines, that induce large quasi-direct current in those lines. When the quasi-direct current travels through the windings of large transformers handling high levels of power, they shift the magnetic field operating point in the core of the transformers, causing the transformer to generate abnormal harmonic waveforms that neither the transformer nor the electrical power system are able to manage. This results in overheating and damage to the transformers. Therefore, it is important that an unclassified bounding-case E3 waveform be available to those working in the commercial power equipment development and operation sectors.

While the DoD has developed high-altitude EMP waveforms (E1, E2, and E3) for its purposes, these are classified and not available for commercial use. The DoD policy of keeping its E3 threat specifications classified, and therefore not available to designers and operators of the U.S. national power grids, is, in the view of the Commission, much more damaging to the protection of U.S. critical national electrical power infrastructure than its release would be helpful to U.S. adversaries. Some potential adversaries, including Russia, have collected some of the

---

<sup>32</sup> T. Phillips. “Near Miss: The Solar Superstorm of July 2012.” Science@NASA, July 23, 2014

best E3 data during their high altitude nuclear tests and therefore are already aware of the magnitude of the E3 fields. The withholding of E3 information is a DoD policy that is neither in the interest of U.S. national security and survival, nor in the interest of the DoD, because the DoD depends on commercial power for many of its activities.

In the absence of an unclassified, well-informed E3 specification, the Commission tasked experts to assess the openly available E3 HEMP measurements from two nuclear high-altitude tests performed by the Soviet Union in 1962. Using these data and an understanding of the scaling relationships for the E3 HEMP heave phenomenon, bounding waveforms for commercial applications were developed.

Because the measured quantities during these tests were the magnetic fields, it is possible for technologists familiar with electromagnetic theory to compute the E3 electric fields, using known ground conductivity profiles. Other ground conductivity profiles could lead to even higher fields, but some of these profiles do not cover a very large area of the Earth.

After computing the electric fields using the Soviet measurements, the results were scaled to account for the fact that the Soviet measurement locations were not at the optimum points on the ground to capture the maximum peak fields. This process determined that the scaled maximum peak E3 EMP heave field would have been 66 volts per kilometer (V/km) for the magnetic latitude of the Soviet tests.

The measured results were also evaluated for the E3 EMP heave field. This parameter increases for burst points closer to the geomagnetic equator, displaying inverse latitude behavior compared to solar GMD fields. This scaling increases the maximum peak electric field up to 85 V/km for locations in the southern continental United States, and 102 V/km for locations near the geomagnetic equator, such as Hawaii. The levels in Alaska would be lower, with a peak value of 38 V/km. While as noted these are not worst-case levels, they are reasonable upper-bound values useful in designing, evaluating, and operating bulk electrical power transmission systems and long-haul copper and fiber communication and data networks.<sup>33</sup>

***Recommendation 4:** The Commission recommends that government agencies and industries adopt new standards to protect critical national infrastructures from damaging E3 EMP heave fields, with more realistic standards of 85 V/km.*

Typical waveforms for commercial applications are included in Appendix B that should prove useful for the protection of the national power grids.

---

<sup>33</sup> Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures*. Report of the EMP Commission, July 2017.



## TESTING SELECTED EMP-VULNERABLE FULL-SYSTEM EQUIPMENT TO FAILURE

Some equipment that is essential for operation of critical infrastructures may be more economically stockpiled and stored in EMP-shielded structures than redesigned to be EMP-hardened. Other equipment with long replacement times or uncertainty of availability after an EMP attack will require EMP-hardening against E1, E2 and E3 hazards. While modeling of EMP vulnerability and mitigation measures is desirable, there is no substitute for full system testing to failure to project the likely post-EMP attack operability or prompt recovery of critical infrastructure equipment.

The Defense Nuclear Agency and its successor Defense Special Weapons Agency sponsored an innovative EMP evaluation program called the Electromagnetic Effects Comparison Test and Reliability Assessment (ELECTRA) from 1992 to 1995. ELECTRA performed both pre-test expert assessments of EMP survivability and system tests to failure using actual threat-level illumination and current injection testing. The ELECTRA Technical Review Group compared sealed-envelope analytical predictions of system EMP effects against post-test system effects.<sup>34</sup> Key findings from ELECTRA are pertinent to development of reliable and cost-effective EMP equipment protection and recovery programs.

The ELECTRA forecasting and test assessment program demonstrated that EMP system effects were most pronounced for modern electronic systems having unprotected external power and signal lines.<sup>35</sup> Moreover, forecasts by EMP survivability experts of pass-fail testing outcomes were no better than random coin-tossing when assessing actual system failures. Predictions of whether or not EMP effects would occur were frequently wrong and predictions for EMP current and voltage stress were subject to large errors (up to +/- 30 dB). System failures were predicted when none occurred, and conversely, no failures were predicted in cases where effects did occur. Pre-test predictions often missed the location—box, component—of system failure. The ELECTRA Technical Review Group concluded that methods used to predict EMP effects in a specific system that are based primarily on analysis or low-level testing are not reliable and recommended,

*Where reliable [electromagnetic effects] predictions for specific systems are required, protections should be based on high-level functional-response tests performed on the specific systems of interest.<sup>36</sup>*

---

<sup>34</sup> The ELECTRA Program's Technical Review Group's interim report of January 1995 includes a set of unclassified chapters on program methodology. See G.H. Baker, P. Castillo, C. McDonald, *et al.*, Electromagnetic Effects Comparison Test and Reliability Assessment (ELECTRA) Program: Executive Summary (U).

<sup>35</sup> ELECTRA Executive Summary (1995), p. iv.

<sup>36</sup> ELECTRA Executive Summary (1995), p. 49.

Further, where one or several complex system samples are subjected to high-level EMP injection testing, the test results can be prudently attributed to the larger population.<sup>37</sup> Thus, threat-level testing of even one sample is helpful to characterize the vulnerability and survivability of the larger set of systems. For large power transformers operating at 345 kV, 500 kV, and 765 kV voltages, for example, the DoD has the capability to transport EMP injection and diagnostic monitoring equipment to sites where these units are deployed. *In situ* testing to failure of exemplars of the major types of large power transformers under load would confirm whether specific types of large power transformers require EMP-protective equipment and enable new type transformer designs that resist EMP effects.

***Recommendation 5:*** *The Commission recommends that the Department of Defense and the Department of Energy provide expedited threat-level, full-system testing of large power transformers in wide use within the bulk electric system and share key findings with the electric utility industry.*

## INTELLIGENCE COMMUNITY ASSESSMENT OF THE EMP THREAT

Finally, the Commission found that the classified report by the Joint Atomic Energy Intelligence Committee (JAEIC) on EMP issued in 2014 is factually erroneous and analytically unsound.<sup>38</sup> We recommend that the DNI circulate to all recipients of the 2014 JAEIC report the EMP Commission critique and direct a new assessment be prepared, reviewed by experts in the subject areas being addressed, and circulated to all the recipients of the 2014 assessment.

***Recommendation 6:*** *The Commission recommends the Director of National Intelligence circulate to all recipients of the 2014 JAEIC report the EMP Commission critique and direct a new assessment be prepared that supersedes the 2014 JAEIC EMP report.*

---

<sup>37</sup> ELECTRA Executive Summary (1995), p. ii

<sup>38</sup> Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *Assessment of the 2014 JAEIC Report on High-altitude EMP Threats*, Report of the EMP Commission, July 2017.

## CONCLUSIONS

---

The critical national infrastructure in the United States faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, as well as from natural EMP from a solar superstorm. During the Cold War, major efforts were undertaken by the Department of Defense to assure that the U.S. national command authority and U.S. strategic forces could survive and operate after an EMP attack. However, no major efforts were then thought necessary to protect critical national infrastructures, relying on nuclear deterrence to protect them. With the development of small nuclear arsenals and long-range missiles by new, radical U.S. adversaries, the threat of a nuclear EMP attack against the U.S. becomes one of the few ways that such a country could inflict devastating damage to the United States. It is critical, therefore, that the U.S. national leadership address the EMP threat as a critical and existential issue, and give a high priority to assuring the leadership is engaged and the necessary steps are taken to protect the country from EMP.

Protecting and defending the national electric grid and other critical infrastructures from cyber and EMP could be accomplished at reasonable cost and minimal disruption to the present systems that comprise U.S. critical infrastructure. The following six recommendations are offered to accomplish this goal.

***Recommendation 1:*** *The Commission recommends the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat.*

***Recommendation 2:*** *The Commission strongly recommends that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection.*

***Recommendation 3:*** *The Commission encourages the President to work with Congressional leaders to establish a joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership to achieve, on an accelerated basis, the protection of critical national infrastructures.*

***Recommendation 4:*** *The Commission recommends that government agencies and industries adopt new standards to protect critical national infrastructures from damaging E3 EMP heave fields, with more realistic standards of 85 V/km.*

***Recommendation 5:*** *The Commission recommends that the Department of Defense and the Department of Energy provide expedited threat-level, full-system testing of large power transformers in wide use within the bulk electric system and share key findings with the electric utility industry.*

***Recommendation 6:*** *The Commission recommends the Director of National Intelligence circulate to all recipients of the 2014 JAEIC report the EMP Commission critique and direct a new assessment be prepared that supersedes the 2014 JAEIC EMP report.*

## APPENDIX A Legislation Re-establishing the Commission

---

**SEC. 1089. REESTABLISHMENT OF COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE ATTACK.**

(a) **REESTABLISHMENT.**—The commission established pursuant to title XIV of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (as enacted into law by Public Law 106-398; 114 Stat. 1654A-345), and reestablished pursuant to section 1052 of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109-163; 50 U.S.C. 2301 note), known as the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, is hereby reestablished.

(b) **MEMBERSHIP.**—Service on the Commission is voluntary, and Commissioners may elect to terminate their service on the Commission. If a Commissioner is unwilling or unable to serve on the Commission, the Secretary of Defense, in consultation with the chairmen and ranking members of the Committees on Armed Services of the House of Representatives and the Senate, shall appoint a new member to fill that vacancy.

(c) **COMMISSION CHARTER DEFINED.**—In this section, the term “Commission charter” means title XIV of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (as enacted into law by Public Law 106-398; 114 Stat. 1654A-345 et seq.), as amended by section 1052 of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109-163; 50 U.S.C. 2301 note) and section 1073 of the John Warner National Defense Act for Fiscal Year 2007 (Public Law 109-364; 120 Stat. 2403).

(d) **EXPANDED PURPOSE.**—Section 1401(b) of the Commission charter (114 Stat. 1654A-345) is amended by inserting before the period at the end the following: “, from non-nuclear EMP weapons, from natural EMP generated by geomagnetic storms, and from proposed uses in the military doctrines of potential adversaries of using EMP weapons in combination with other attack vectors.”.

(e) **DUTIES OF COMMISSION.**—Section 1402 of the Commission charter (114 Stat. 1654A-346) is amended to read as follows:

**“SEC. 1402. DUTIES OF COMMISSION.**

“The Commission shall assess the following:

“(1) The vulnerability of electric-dependent military systems in the United States to a manmade or natural EMP event, giving special attention to the progress made by the Department of Defense, other Government departments and agencies of the United States, and entities of the private sector in taking steps to protect such systems from such an event.

“(2) The evolving current and future threat from state and non-state actors of a manmade EMP attack employing nuclear or non-nuclear weapons.

“(3) New technologies, operational procedures, and contingency planning that can protect electronics and military systems from the effects of a manmade or natural EMP event.

“(4) Among the States, if State grids are protected against manmade or natural EMP, which States should receive highest priority for protecting critical defense assets.

“(5) The degree to which vulnerabilities of critical infrastructure systems create cascading vulnerabilities for military systems.”.

(f) **REPORT.**—Section 1403 of the Commission charter (114 Stat. 1654A-345) is amended by striking “September 30, 2007” and inserting “June 30, 2017”.

(g) **TERMINATION.**—Section 1049 of the Commission charter (114 Stat. 1654A-348) is amended by inserting before the period at the end the following: “, as amended by the National Defense Authorization Act for Fiscal Year 2016”.



## APPENDIX B High Altitude Nuclear Explosion-Generated Electromagnetic Effects

---

In the case of high altitude nuclear bursts, three main phenomena come into play, each with distinct associated system effects:

1. The first, a “prompt” EMP field, also referred to as E1, is created by gamma ray interaction with stratospheric air molecules. It peaks at tens of kilovolts per meter in a few nanoseconds, and lasts for a few hundred nanoseconds. E1’s broad-band power spectrum (frequency content in the 10s to 100s of megahertz) enables it to couple to electrical and electronic systems in general, regardless of the length of their penetrating cables and antenna lines. Induced currents range into the 1000s of amperes. Exposed systems may be upset or permanently damaged.
2. The second component of the EMP field, referred to as E2, is produced by delayed gamma rays and neutron-induced currents, lasts from microseconds to milliseconds, and has a magnitude in the hundreds of volts per meter. Its spectral characteristics are similar to those of naturally occurring lightning.
3. The third component, late-time EMP, also referred to as magnetohydrodynamic (MHD) EMP or E3, is caused by the distortion of the earth’s magnetic field lines due to the expanding nuclear fireball and rising of heated and ionized layers of the ionosphere. The change of the magnetic field at the earth’s surface induces currents of 100s-1000s of amperes in long conducting lines (a few kilometers or greater) that damage components of the electric power grid itself as well as connected systems. Long-line communication systems are also affected, including copper as well as fiber-optic lines with repeaters. Transoceanic cables are a prime example of the latter.

Solar storm geomagnetic disturbance (GMD) effects are the result of large excursions in the flux levels of charged particles from the Sun and their interactions with the Earth’s magnetic field and upper atmosphere. Perturbation of the Earth’s magnetic field, similar to MHD EMP, can generate overvoltages in long-line systems over large regions of the earth’s surface affecting electric power and communication transmission networks.

For each effect, directly-affected systems may be upset or permanently damaged. For unmanned systems and industrial control systems, upset effects can cascade to cause permanent damage to other connected systems. Wide-area electromagnetic system effects are challenging due to their near-simultaneous initial effects and cascading effects on a wide array of infrastructures. Infrastructure systems comprised of long-line conductor networks are the most vulnerable to both effects. Susceptible networks include the electric power grid, land-line communications, and interstate pipelines. Effects on these networks will cascade to most other



infrastructures. Smaller, self-contained, self-powered infrastructure systems (e.g. hand-held radios and vehicles) are also directly vulnerable, but only to EMP (not GMD) and to a lesser degree than long-line networks.

## BIOGRAPHIES

---

### COMMISSIONERS

**Dr. William R. Graham** is Chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. He was Chairman of the Board and Chief Executive Officer of National Security Research Inc. (NSR), a Washington-based company that conducts technical, operational, and policy research and analysis related to US national security. Previously he served as a member of several high-level study groups, including the Department of Defense Transformation Study Group, the Defense Science Board, the Commission to Assess United States National Security Space Management and Organization (the Rumsfeld Commission on Space), the Commission to Assess the Ballistic Missile Threat to the United States (also led by Hon. Donald Rumsfeld), and the National Academies' Board on Army Science and Technology. From 1986–89 Dr. Graham was the Director of the White House Office of Science and Technology Policy while he served concurrently as Science Advisor to President Reagan, Chairman of the Federal Joint Telecommunications Resources Board, and member of the Arms Control Experts Group. Before going to the White House, he served as the Deputy Administrator of NASA. For 11 years, he served as a member of the Board of Directors of the Watkins-Johnson Company.

**Dr. John S. Foster, Jr.** began his career at the Radio Research Laboratory of Harvard University in 1942 and then volunteered to be an advisor to the 15th Army Air Force on radar countermeasures in Italy. In 1952, Dr. Foster joined the Lawrence Livermore National Laboratory, designed nuclear weapons, became Director of that Laboratory, then in 1965 served as Director of Defense Research and Engineering for the Department of Defense until 1973. He joined TRW to work on energy programs and then served on the Board, retiring in 1988. He currently serves as a consultant to LLNL and an Advisor to STRATCOM SAG Panel. He has served on the Air Force Scientific Advisory Board, Army Scientific Advisory Panel, Ballistic Missile Defense Advisory Committee, and Advanced Research Projects Agency. From 1973 – 1990 he was a member of the President's Foreign Intelligence Advisory Panel. He served as Chairman of the Defense Science Board from 1990 to 1993. He served on the Congressional Commission on the Strategic Posture of the United States and on the Advisory Committee to the Director of DARPA.

**Mr. Earl Gjelde, P.E.**, is the Managing Director and Chief Executive Officer of Summit Group International, Ltd.; Summit Energy Group, Ltd.; Summit Energy International 2000, LLC; and Summit Power NW, LLC, primary participants in the development of over 5,000 megawatts of natural gas fired electric and wind generating plants within the United States. He has also held a number of government posts, serving as President George Herbert Walker Bush's Under (now called Deputy) Secretary and Chief Operating Officer of the US Department of the Interior (1989) and as President Ronald Reagan's Under Secretary and Chief Operating Officer of the US Department of the Interior (1985–1988). While in the Reagan administration he served

concurrently as Special Envoy to China (1987), Deputy Chief of Mission for the US-Japan Science and Technology Treaty (1987–1988), and Counselor for Policy to the Director of the National Critical Materials Council (1986–1988); the Counselor to the Secretary and Chief Operating Officer of the US Department of Energy (1982-1985); and Deputy Administrator, Chief Operating Officer, and Power Manager of the Bonneville Power Administration (1980-1982). Prior to 1980, he was a principal officer of the Bonneville Power Administration.

**Dr. Robert J. Hermann** is a senior partner of Global Technology Partners, LLC, a Boston-based investment firm that focuses on technology, defense aerospace, and related businesses worldwide. In 1998, Dr. Hermann retired from United Technologies Corporation, where he was Senior Vice President, Science and Technology. Prior to joining UTC in 1982, Dr. Hermann served 20 years with the National Security Agency with assignments in research and development, operations, and NATO. In 1977, he was appointed Principal Deputy Assistant Secretary of Defense for Communications, Command, Control, and Intelligence. In 1979, he was named Assistant Secretary of the Air Force for Research, Development, and Logistics and concurrently was Director of the National Reconnaissance Office.

**Mr. Henry (Hank) M. Kluepfel** served as Vice President for Corporate Development at SAIC, where he was the company's leading cyberspace security advisor to the President's National Security Telecommunications Advisory Committee (NSTAC) and the Network Reliability and Interoperability Council (NRIC). Mr. Kluepfel is widely recognized for his 30-plus years of experience in security technology research, design, tools, forensics, risk reduction, education, and awareness, and he is the author of industry's de facto standard security base guideline for the Signaling System Number 7(SS7) networks connecting and controlling the world's public telecommunications networks. In past affiliations with Telcordia Technologies (formerly Bellcore), AT&T, BellSouth and Bell Labs, he led industry efforts to protect, detect, contain, and mitigate electronic and physical intrusions and led the industry's understanding of the need to balance technical, legal, and policy-based countermeasures to the then emerging hacker threat. He has been recognized as a Certified Protection Professional by the American Society of Industrial Security and is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

**Gen Richard L. Lawson, USAF (Ret.),** served as Chairman of Energy, Environment and Security Group, Ltd., and as President and CEO of the National Mining Association. He also served as Vice Chairman of the Atlantic Council of the U.S.; Chairman of the Energy Policy Committee of the US Energy Association; Chairman of the United States delegation to the World Mining Congress; and Chairman of the International Committee for Coal Research. Active duty positions included serving as Military Assistant to the President; Commander, 8th Air Force; Chief of Staff, Supreme Headquarters Allied Powers Europe; Director for Plans and Policy, Joint Chiefs of Staff; Deputy Director of Operations, Headquarters US Air Force; and Deputy Commander in Chief, US European Command.

**Dr. Gordon K. Soper** served as the Group Vice President of Defense Group Inc., responsible for broad direction of corporate goals relating to company support of government customers in

areas of countering the proliferation of weapons of mass destruction, chemical/biological defense and domestic preparedness, treaty verification research, nuclear arms control and development of new business areas and growth of technical staff. He has also provided senior-level technical support on a range of task areas to the Defense Threat Reduction Agency (DTRA), the Chemical and Biological National Security Program of National Nuclear Security Administration, and the Counterproliferation and Chem/Bio Defense Office of the Office of the Secretary of Defense. Previously, Dr. Soper was Principal Deputy to the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Programs (ATSD (NCB); Director, Office of Strategic and Theater Nuclear Forces Command, Control and Communications (C3) of the Office of the Assistant Secretary of Defense (C3I); and Associate Director for Engineering and Technology/Chief Scientist at the Defense Communications Agency.

**Dr. Lowell L. Wood, Jr.** is retired from a career-long position on the technical staff of Lawrence Livermore National Laboratory, operated by the University of California for the U.S. Department of Energy, and an extended term as a Research Fellow of the Hoover Institution at Stanford University. Since his retirement a decade ago, Dr. Wood has continued part-time technical consulting in the commercial sector and serving as an External Advisor of the Bill & Melinda Gates Foundation, the world's largest private charity, focusing his efforts on global health and development. Dr. Wood holds the distinction of being the most inventive American in history, holding more U.S. patents on new inventions than any other person, including Thomas Edison, the previous record-holder.

**Dr. Joan Woodard** was Executive Vice President and Deputy Director of Sandia National Laboratories, responsible for all of Sandia's programs, operations, staff, and facilities. She was also responsible for the laboratory's strategic planning. Previously, Dr. Woodard was Vice President of the Energy, Information and Infrastructure Technology Division, where her responsibilities included energy-related projects in fossil energy, solar, wind, geothermal, geosciences, fusion, nuclear power safety and severe accident analysis, and medical isotope processing; environment-related programs in remediation, nuclear waste management and repository certification, and waste minimization; information technology programs in information surety, command and control systems, and distributed information systems; and programs responsible for security of the transportation of nuclear weapons and special nuclear materials, and safety of commercial aviation. Over 80 percent of the programs included industrial or academic partners, and the nature of the work ranged from basic research to prototype systems evaluation.

## SENIOR ADVISORS

**Dr. George H. Baker** is a Professor Emeritus at James Madison University, where he directed the JMU Institute for Infrastructure and Information Assurance. Previously, Dr. Baker led the Defense Nuclear Agency's Electromagnetic Pulse (EMP) program, directed the Defense Threat Reduction Agency's assessment arm, and served as a member of the Congressional EMP

Commission Staff. Dr. Baker holds an M.S. in Physics from University of Virginia, and a Ph.D. in Engineering Physics from the U.S. Air Force Institute of Technology. Currently, Dr. Baker is CEO of BAYCOR, LLC, and is Director of the Foundation for Resilient Societies.

**Mr. William R. Harris** is an international lawyer specializing in arms control, nuclear non-proliferation, energy policy, and continuity of government. He worked on Hot Line upgrades, creation of linked Nuclear Risk Reduction Centers, and was a co-drafter of arms limitation treaties in 1986-87, 1991, and 1993. Mr. Harris worked for the RAND Corporation and in a variety of assignments for the U.S. Government. Mr. Harris holds a B.A. from Harvard College and a J.D. from Harvard Law School. Mr. Harris serves as Secretary and attorney for the Foundation for Resilient Societies.

**Dr. Peter Vincent Pry** is a recognized expert on protection strategies for electromagnetic pulse (EMP) and related threats. In addition to his service for the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, he has served on the Congressional Strategic Posture Commission, as Executive Director of the U.S. Nuclear Strategy Forum and the Task Force on National and Homeland Security (both Congressional Advisory Boards); as Professional Staff on the House Armed Services Committee of the U.S. Congress, with portfolios in nuclear strategy, WMD, Russia, China, NATO, the Middle East, intelligence, and terrorism; as an Intelligence Officer with the Central Intelligence Agency; and as a Verification Analyst at the U.S. Arms Control and Disarmament Agency. Dr. Pry has written numerous books and articles on national security issues.

**Dr. William A. Radasky** is President and Managing Engineer at the Metatech Corporation. Metatech develops technically sound and innovative solutions to problems in all areas of electromagnetic environmental effects, including: electromagnetic interference and compatibility, geomagnetic storm assessments and protection, nuclear electromagnetic pulse prediction, assessments, protection and standardization, and intentional electromagnetic interference assessments, protection and standardization. Dr. Radasky has published over 400 technical papers, reports and articles dealing with electromagnetic interference (EMI) and protection. In 2004 he received the Lord Kelvin Award from the International Electrotechnical Commission for exceptional contributions to international standardization.

**Dr. David Stoudt** is a Senior Executive Advisor at Booz Allen where he provides leadership and guidance on the science and business of advancing directed energy capabilities for American warfighters. He previously spent 32 years serving in the Department of Navy, with deep experience in directed energy and electric weapon systems, including high-energy lasers, the electromagnetic rail gun, and high-power microwave weapon systems. Among other honors, David has received multiple Meritorious Civilian Service Awards, the Navy Distinguished and Superior Civilian Service Awards, and the Naval Sea Systems Command Scientist of the Year Award.

**Ambassador R. James Woolsey Jr., J.D.**, is a national security and energy specialist and former Director of Central Intelligence who headed the Central Intelligence Agency from

February 5, 1993, until January 10, 1995. A lawyer by training and trade, he held a variety of government positions in the 1970s and 1980s, including as Under Secretary of the Navy from 1977 to 1979, and was involved in treaty negotiations with the Soviet Union for five years in the 1980s, including as Chief Negotiator of the Conventional Forces in Europe Treaty.



## COMMISSION REPORTS

---

### REPORTS OF THE COMMISSION

Executive Report, 2004

Critical National Infrastructures Report, 2008

Assessing the Threat from EMP Attack: Executive Report, 2017

Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures, 2017

Assessment of the 2014 JAEIC Report on High-altitude Electromagnetic Pulse (HEMP) Threats,  
**SECRET//RD-CNWDI//NOFORN**, 2017

### STAFF PAPERS TO THE COMMISSION

G. Baker. Risk-Based National Infrastructure Protection Priorities for EMP and Solar Storms, 2017

W.R. Graham. Chairman's Report, 2017.

J. G. Kappenman and W.A. Radasky. Examination of NERC GMD Standards and Validation of Ground Models and Geo-Electric Fields, 2017

T.S. Popik, G.H. Baker, and W.R. Harris. Electric Reliability Standards for Solar Geomagnetic Disturbances, 2017

P.V. Pry. Nuclear EMP Attack Scenarios and Combined-arms Cyber Warfare, 2017

P.V. Pry. Political-Military Motives for Electromagnetic Pulse Attack, 2017

P.V. Pry. Foreign Views of Electromagnetic Pulse Attack, 2017

P.V. Pry. Life without Electricity: Storm Induced Blackouts and Implications for Electromagnetic Pulse Attack, 2017

P.V. Pry. Nuclear Terrorism and Electromagnetic Pulse Attack, 2017

E. Savage and W. Radasky. Late-Time (E3) HEMP Heave Parameter Study, **SECRET//RD**, 2017

# **LIFE WITHOUT ELECTRICITY: STORM-INDUCED BLACKOUTS AND IMPLICATIONS FOR EMP ATTACK**

by

Dr. Peter Vincent Pry

July 2017

Report to the Commission to Assess the Threat to the United States  
from Electromagnetic Pulse (EMP) Attack

REPORT TO THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES  
FROM ELECTROMAGNETIC PULSE (EMP) ATTACK

---

**LIFE WITHOUT ELECTRICITY:  
STORM-INDUCED BLACKOUTS AND  
IMPLICATIONS FOR EMP ATTACK**

by

**Dr. Peter Vincent Pry**

**July 2017**

This paper was drafted on June 20, 2003 to inform the work of the EMP Commission during 2001-2008, but could not be published because the Commission was terminated before Staff Papers could be submitted for security classification review. It is offered now for completeness of the analytical record.

The cover photo depicts Fishbowl Starfish Prime at 0 to 15 seconds from Maui Station in July 1962, courtesy of Los Alamos National Laboratory.

This report was produced to support the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. The Commission was established by Congress in the FY2001 National Defense Authorization Act, Title XIV, and was continued per the FY2016 National Defense Authorization Act, Section 1089.

The Commission completed its information-gathering in June 2017. The report was cleared for open publication by the DoD Office of Prepublication and Security Review on October 19, 2017.

This report is unclassified and cleared for public release.

**Table of Contents**

Summary .....2

Hurricane Lili (October 2002).....5

Hurricane Floyd (September 1999) .....7

Ice Storm Washington, D.C. (14 January 1999) .....8

The Great Ice Storm (January 1998).....9

Western Heat Wave (10 August 1996) .....12

Hurricane Andrew (August 1992) .....15

## Summary

Storm-induced blackouts of the electric power grid are suggestive of the possible consequences of an electromagnetic pulse (EMP) attack, such as could be made by rogue states or terrorists detonating a nuclear weapon at high-altitude over the United States. Electric power grid failure caused by storms cascade through other critical infrastructures—such as communications, transportation, emergency medical services, food and water supply systems. Storm-induced blackouts provide an objective basis for extrapolating judgments about the threat posed by EMP to the civilian infrastructures that sustain economic, political, and social life.

The vulnerability of critical infrastructures to various forms of attack has been a growing concern in recent years, drawing presidential attention in the Marsh Commission, and receiving additional impetus after the terrorist attacks of September 11<sup>th</sup> that moved President Bush to establish the Department of Homeland Security. However, the science of analyzing critical infrastructures, their interdependencies, and their possible vulnerabilities is relatively new. Much effort and significant resources have been invested in an inductive approach to understanding the potential for cascading failures through the critical infrastructures that may result from failure of the power grid. The prevailing approach relies heavily on complex mathematical calculations, theoretical models, and computer simulations.

Analysis of storm-induced blackouts and their consequences offers an empirical approach that complements the predominant inductive approach to understanding infrastructure interdependence and vulnerability. Moreover, beyond the interdependence and potential vulnerability of critical infrastructures, analysis of storm-induced blackouts provides some empirical basis for estimating the effects of infrastructure failure on social order.

Storm-induced blackouts are an imperfect analogy to EMP attack from nuclear weapons of high-yield or special design. Taken at face value, storm-induced blackouts and their consequences grossly understate the threat posed by EMP attack. Storms are much more limited in geographic scope compared to EMP attack. So power grid recovery from storms, compared to recovery from EMP attack, is likely to be faster because of the “edge effect”—the capability of neighboring localities and states to provide recovery assistance. Because EMP attack is likely to damage or disrupt electronics over a much wider geographic area than storm-induced blackouts, rescuers from neighboring states and localities would face a much bigger job, and recovery probably would take a much longer time.

Nor do storm-induced blackouts replicate the damage from an EMP attack that may occur in small-scale electronic systems such as computers, aircraft, and automobiles. Compared to storms, nuclear weapons of high-yield or special design are likely to inflict, not only more widespread damage geographically, but deeper damage, affecting a much broader spectrum of electronic equipment.

Storms are merely suggestive of, and provide some basis for extrapolating, the greater destructive effects on infrastructures and social order by an EMP attack from a nuclear weapon



of high-yield or special design. Storm-induced blackouts and their consequent physical damage to other infrastructures may well be equivalent to an EMP attack from a nuclear weapon of low-yield and primitive design, such as terrorists might be able to build. In this latter case, storm-induced blackouts and the cascading physical effects on other infrastructures may be taken as representative of the lowest, and most benign, level of the EMP threat spectrum.

However, although some storms may be equivalent to a primitive EMP attack in their physical damage to the power grid and other infrastructures, storms probably understate even a primitive EMP attack in its psychological dimensions. Unlike EMP attack, hurricanes and other storms are familiar to the public and understood to be acts of nature, not the destructive agents of a foreign enemy. Public perceptions of and reactions to mass destruction differ markedly when the agent of destruction is a familiar natural event or accident, versus destruction by unfamiliar means inflicted deliberately by malignant actors. For example, the American people endure tornadoes and hurricanes without mass panic, and accept with equanimity 50,000 deaths yearly from automobile accidents. But the same number of deaths inflicted over a decade by a foreign enemy was enough to cause a political and cultural revolution in the United States, and broke the will of the people and political elites who accepted defeat in the Vietnam War. More recently, the 3,000 deaths and other destruction inflicted by the terrorist attacks of September 11 have moved the United States, with wide popular support, to prosecute successful wars in Afghanistan and Iraq as part of a broader ongoing war against terrorism. The United States government and people support this effort because, although U.S. society can survive the worst hurricane, the September 11 events forged a new consensus that U.S. society, and civilization itself, may not be able to survive future terrorist attacks.

Psychologically benign though storms may be, compared to terrorist attacks that inflict lesser or greater physical destruction, even storms challenge social order. This survey has found that some storm-induced blackouts have caused crime waves and disintegrated organized communities into disorganized refugees, for example.

Significantly, some observers of storm-induced blackouts—even when blackouts lasted only a day or two, as is commonly the case—were struck by the potential fragility of modern society and its near total dependence upon electricity. For example, a January 1999 ice storm that blacked-out electricity in the Washington, D.C. area moved the **Washington Post** to note that “daily life was crippled, if not halted—dramatically illustrating the fragile dependence of modern times on the flip of a switch.”<sup>1</sup> The *Post* continued:

*Automated teller machines were out, as were gasoline pumps at many service stations. WETA-TV (Channel 26) went black for more than 10 hours until employees found a diesel generator to put that station back on the air. The Montgomery County jail conducted bond hearings by flashlight. Families seeking refuge at Tysons Corner Center were booted out at 6 p.m. because of*

---

<sup>1</sup> Susan Levine and Tom Jackman, “Region Iced Over and Blacked Out,” **Washington Post** (16 January 1999), p. A1.

*water problems at the mall....Up and down Metro's Red Line, riders confronted stalled elevators, inoperable Farecard machines and even closed stations. Negotiating roads...was often no easier. Of more than 700 traffic signals in Montgomery, 430 were dead. Across the area, but especially in Montgomery, hotels filled to capacity with customers fleeing cold, dark homes. The 365-room Doubletree Hotel on Rockville Pike was sold out by 8 a.m.....Other residents, with pioneering spirit, decided to ride out the outage. More than two dozen people were waiting when the Home Depot in Germantown opened at 6 a.m.. By 10 a.m., the store had sold every generator, log of firewood, candle, kerosene heater and any other supply that could warm hands and feet.<sup>2</sup>*

Another dramatic example of the dependency of social order upon electricity occurred in October 2002, during the aftermath of Hurricane Lili that blacked-out much of coastal Louisiana. In some areas, the absence of street lights caused "looting and vandalism bad enough to require enforcement of a dusk-to-dawn curfew."<sup>3</sup> Local police had to be reinforced by police from neighboring localities in order to cope with the crime wave. "The looting," remarked Abbeville Mayor Mark Piazza, "Is not expected to go away until the lights come on."<sup>4</sup>

Some experts claim that an EMP attack that collapses the power grid would, in effect, return society to a pre-industrial condition. A February 1987 snowstorm that blacked-out the Washington, D.C. area suggested exactly this to many of its victims. According to press reports, people were reduced to using open fires for heat, cooking and, in some areas, melting snow for water. Homes with fireplaces became havens for multiple families seeking refuge from houses heated by electric, gas, or oil that no longer worked. As she "stoked a fire and began sterilizing water for her baby's formula," one woman told reporters, "It's like the Colonial days."<sup>5</sup>

Storm-induced blackouts are localized and last usually no more than a day or two. Yet they can momentarily return part of our society to technological primitivism and begin cracks in the social order. Compared to storms, the consequences of an EMP attack would be far graver. Compared to the worst storms, an EMP attack would probably destroy infrastructures more completely within a region and over a much larger region—perhaps over the entire continental United States. An EMP attack, compared to the worst storms, would probably inflict more lasting damage—requiring perhaps weeks or months to repair.

Therefore, we can reasonably infer from the data on storm-induced blackouts and the known greater severity of high-altitude nuclear EMP that the consequences of an EMP attack on the United States' infrastructures and society would be an unprecedented and first order catastrophe.

---

<sup>2</sup> Ibid.

<sup>3</sup> Leslie Williams, "One Town's Battle," **Times-Picayune** (9 October 2002), p. 1.

<sup>4</sup> Ibid.

<sup>5</sup> John Lancaster and Chris Spolar, "Washington's Wet Blanket," **Washington Post** (24 February 1987), p. 1.

Some of the salient infrastructure and social consequences of storm-induced blackouts are listed below. Not all of the failures and effects described occurred during all storms. This survey was careful to select only failures and effects traceable to power grid failure. Failures and effects resulting from phenomenon other than electric power grid blackout (downed trees, flooding and etc.) are not reported here. Storm- and weather-related blackouts examined in this survey include Hurricane Lili (2002), Hurricane Floyd (1999), the Washington Ice Storm of 1999, the Great Ice Storm of 1998, the Western Heat Wave of 1996, and Hurricane Andrew (1992):

- **Social Order:** Looting requires dusk to dawn curfew. People become refugees as they flee powerless homes. Work force becomes differently employed at scavenging for basics, including water, food, and shelter.
- **Communications:** No TV, radio, or phone service.
- **Transportation:** Gas pumps inoperable. Failure of signal lights and street lights impedes traffic, stops traffic after dark. No mass transit metro service. Airlines stopped.
- **Water and Food:** No running water. Stoves and refrigerators inoperable. People melt snow, boil water, and cook over open fires. Local food supplies exhausted. Most stores close due to blackout.
- **Energy:** Oil and natural gas flows stop.
- **Emergency Medical:** Hospitals operate in dark. Patients on dialysis and other life support threatened. Medications administered and babies born by flashlight.
- **Death and Injury:** Casualties from exposure, carbon dioxide poisoning and house fires increase.
- **Edge Effect:** Recovery depends heavily on neighboring regions unaffected by blackout. For example, Louisiana rescued from Hurricane Lili blackout by 14,000 workers from 24 states.

### **Hurricane Lili (October 2002)**

Hurricane Lili struck the coast of Louisiana on October 3, 2002, coming ashore at Vermillion Bay, the eye of the storm centered on Abbeville about 90 minutes after landfall.<sup>6</sup> Lili knocked down 35 transmission lines and destroyed 53 electric power substations.<sup>7</sup> More than 500,000 people were without electric power at the height of the blackout, immediately after the storm.<sup>8</sup> Three days later, on October 6, over 100,000 homes and businesses were still without power in coastal Louisiana, according to the state Office of Emergency Preparedness.<sup>9</sup> Six days after Lili, on October 9, in Abbeville and surrounding Vermillion Parish, an estimated 80 percent of the 20,000 homes and 50 percent of businesses were still without electricity.<sup>10</sup>

---

<sup>6</sup> Williams, op. cit., p. 1.

<sup>7</sup> Angela Simoneaux, "Flooded, Battered La. Gets Busy Cleaning Up," **Morning Advocate** (5 October 2002), p. 1A.

<sup>8</sup> Angela Simoneaux, "Acadiana's Recovery," **The Advocate** (8 October 2002), p. 5B.

<sup>9</sup> Kevin McGill, "Rise Seen In Carbon Monoxide Poisoning Cases," **The Advocate** (7 October 2002), p. 2B.

<sup>10</sup> Williams, op. cit., p. 1.

As a consequence of the blackout, water and food were unavailable through the normal means to thousands. With no electricity, water pumping stations no longer worked. In south Louisiana, 30 supermarkets would not open because the blackout prevented their cash registers from operating. Those grocery stores that did open were stripped of food within hours. In Abbeville, the parking lots of shopping centers became watering and feeding stations run by churches and the state Office of Emergency Preparedness. Associated Grocers, that supplies food to supermarkets in Louisiana, Texas, and Mississippi, sent food and refrigerated trucks to the stricken area. The food emergency was reflected in a skyrocketing demand for dry ice to preserve food stuffs during the hot weather and to preserve refrigerated foods. Local supplies of dry ice were exhausted—one store selling 20,000 pounds of dry ice to hundreds of customers in two hours—and had to be supplemented with supplies from the Red Cross.<sup>11</sup>

The electrical outage deprived thousands of phone service for days after the Hurricane.<sup>12</sup> Television service was also blacked out.<sup>13</sup>

The blackout interfered with transportation by rendering signal lights inoperable.<sup>14</sup> Street lights were also inoperable, making driving at night difficult even for long-time local residents, who could not see landmarks and became disoriented in the dark.<sup>15</sup>

Power grid collapse caused failure in other energy infrastructures. Without electricity, natural gas service could not be restored for several days after Lili.<sup>16</sup>

Many hospitals were plunged into darkness during the blackout because they had no emergency generators or emergency power systems failed to work. There was no hot water for bathing patients or sterilization. “We have to give them medicines in the dark,” said one nurse, “We use a flashlight to make sure we don’t give them the wrong one.”<sup>17</sup>

The blackout caused indirectly some injuries and at least one death. Home generators used by people who lost power after Hurricane Lili led to more than 60 cases of carbon monoxide poisoning, including one fatality, according to Louisiana health officials.<sup>18</sup>

Some officials and citizens considered the blackout the worst part of Hurricane Lili. According to Mayor Chuck Butterfield, “We’ve taken electricity for granted and living without it for three or four days is devastating.”<sup>19</sup> Law enforcement officers blamed a surge of looting and vandalism on the blackout. The crime wave became bad enough to require the imposition of a dusk-to-dawn curfew and police reinforcements from neighboring areas unaffected by the storm.

---

<sup>11</sup> Simoneaux, “Acadiana’s Recovery,” p. 5B. Williams, op. cit., p. 1. Simoneaux, “Flooded, Battered La. Gets Busy Cleaning Up,” p. 1A. Suzan Manuel, “Lili Leaves Residents Powerless,” *Daily Town Talk* (5 October 2002), p. 1A. Suzan Manuel, “Thousands Still Without Electricity Across Central La.,” *Daily Town Talk* (6 October 2002), p. 8A.

<sup>12</sup> McGill, op. cit., p. 2B.

<sup>13</sup> Simoneaux, “Acadiana’s Recovery,” p. 5B.

<sup>14</sup> Manuel, “Lili Leaves Residents Powerless,” p. 1A.

<sup>15</sup> Williams, op. cit., p. 1.

<sup>16</sup> McGill, op. cit., p. 2b.

<sup>17</sup> Manuel, “Lili Leaves Residents Powerless,” p. 1A.

<sup>18</sup> McGill, op. cit., p. 2B.

<sup>19</sup> Manuel, op. cit. p. 8A.

“The looting,” according to the Abbeville Sherriff’s Office, “Is not expected to go away until the lights come back on.”<sup>20</sup>

Recovery from the blackout, described by a CLECO electric utility spokesman as “the biggest customer outage event in our history,” depended heavily on outside assistance.<sup>21</sup> Some 14,000 electric utility workers from 24 states and the District of Colombia joined CLECO’s 3,000 workers to make recovery possible in about one week.<sup>22</sup>

### **Hurricane Floyd (September 1999)**

Expected to be a “killer storm” of rare power and destruction, when Hurricane Floyd made landfall near Cape Fear, North Carolina on September 16, 1999, it had subsided into a tropical storm that inundated much of the east coast with heavy rainfall and flooding. But there was little of the destruction anticipated by federal and state authorities that had prompted them to evacuate over 3 million people from the hurricane’s path.<sup>23</sup>

Floyd did blackout electrical grids in many areas. However, the consequences of those blackouts for other infrastructures and for society are difficult to evaluate since blackouts tended to occur in areas where the population had already evacuated. Blackouts did interrupt phone service in North Carolina.<sup>24</sup> In Salisbury, North Carolina, more than 200 of 1,200 supermarkets were put out of operation by protracted blackouts, causing substantial food spoilage despite emergency efforts undertaken before the storm to preserve perishable goods in freezers.<sup>25</sup> Most cable TV customers lost service in Baltimore due to a blackout.

Floyd blackouts are notable for causing water treatment and sewage plants to fail in some Virginia localities and, most notably, in Baltimore. Blackout induced failure of Baltimore’s Hampden sewage facility for several days raised concerns about a threat to public health. With its three pumps inoperable, Hampden spilled 24 million gallons of waste into Baltimore’s Jones Falls waterway and the Inner Harbor.<sup>26</sup>

Perhaps Floyd’s blackouts are most significant for complicating the largest evacuation and return of civilians in United States history. Electrical outages apparently prevented many from finding shelter—some traveled over 500 miles seeking accommodations, and found none. Blackout induced failure of traffic signals contributed to some of the largest traffic jams in the

---

<sup>20</sup> Williams, op. cit., p. 1.

<sup>21</sup> Simoneaux, “Flooded, Battered La. Gets Busy Cleaning Up,” p. 1A.

<sup>22</sup> Keith Darce, “Lights Blink Out All Over Louisiana,” **Times-Picayune** (4 October 2002), p. 1. “Lili Left Half A Million Without Power,” **Associated Press** (4 October 2002).

<sup>23</sup> Brad Liston, Melissa August, Delphine Matthieussent, and Timothy Roche, “A Very Close Call,” **Time** (27 September 1999), p. 34.

<sup>24</sup> Amanda Milligan Hoffman and Sally Roberts, **Business Insurance** (Crain Communications: 1999).

<sup>25</sup> Ibid.

<sup>26</sup> Governors James Hunt and James Gilmore interviewed, “Hurricane Floyd Leaves Lingering Questions About Public Policy,” **CNN Crossfire** (16 September 1999). Del Quentin Wilber, “Jones Falls Sewage Spill Lasts 2 Days,” **Baltimore Sun** (19 September 1999), p. 1A.

nation's history as evacuees tried to return home. For example, one traffic jam on Interstate 10 from the Carolinas to Florida stretched 200 miles.<sup>27</sup>

### **Ice Storm Washington, D.C. (14 January 1999)**

On January 14, 1999, an ice storm downed 250 high-voltage power lines in Washington D.C. and the neighboring suburbs in Maryland and Northern Virginia, causing what the Potomac Electric Power Company (PEPCO) described as "the worst power outage in the utility's 102-year history."<sup>28</sup> The blackout left 435,000 homes and businesses without power. Recovery took six days.<sup>29</sup>

Warm food, potentially a survival issue in the freezing winter conditions, was not available in most people's homes because electric ovens and microwaves no longer worked. Most gas-powered ovens also would not work because those built since the mid-1980s have electronic ignition and cannot be lit with a match.<sup>30</sup> Some resorted to cooking on camp stoves. Preserving refrigerated foods was also a concern that PEPCO tried to help address by giving away 120,000 pounds of dry ice, all it had.<sup>31</sup> Dry ice became a precious commodity.<sup>32</sup>

The blackout crippled ground and rail transportation. Gasoline pumps were rendered inoperable. Non-functioning traffic lights snarled traffic:

*Up and down Metro's Red Line, riders confronted stalled elevators, inoperable fare card machines and even closed stations. Negotiating roads...was often no easier. Of more than 700 traffic signals in Montgomery, 430 were dead....Arlington County motorcycle officers proved especially resourceful, borrowing portable generators from the public library system to help run traffic lights at four major intersections.*<sup>33</sup>

A local television station, WETA-TV, went off the air for more than 10 hours because of the blackout.<sup>34</sup>

At least one hospital was blacked out. Babies were born by flashlight.<sup>35</sup> Emergency medical services suffered to such an extent that patients requiring life support were put at risk, PEPCO admitted:

<sup>27</sup> Liston and et. al., op. cit., p. 34. Aaron Steckelberg, "Scenes From The Coast," **Atlanta Constitution** (16 September 1999), p. 10A.

<sup>28</sup> Scott Wilson, "From Ice Storm To Firestorm," **Washington Post** (31 January 1999), p. A1. Manuel Perez-Rivas, "Six-Day Power Outage Is Over," **Washington Post** (21 January 1999), p. B1.

<sup>29</sup> Ibid.

<sup>30</sup> Phillip P. Pan and Spencer S. Hsu, "Without Power, Thousands Wait In Hotels, Malls And Cold Homes," **Washington Post** (17 January 1999), p. A1.

<sup>31</sup> Perez-Rivas, op. cit., p. B1.

<sup>32</sup> Wilson, op. cit. (31 January 1999), p. A1.

<sup>33</sup> Susan Levine and Tom Jackman, "Region Iced Over and Blacked Out," **Washington Post** (16 January 1999), p. A1.

<sup>34</sup> Ibid.

<sup>35</sup> Wilson, op. cit. (31 January 1999), p. A1.



*The extent of damage caused by last week's ice storm prevented PEPCO and other area utilities from giving priority to customers with serious medical conditions, including those on life-support systems or dialysis machines, company executives said yesterday.*<sup>36</sup>

Ice storm induced blackout in freezing conditions posed a threat to life. Hypothermia surged among the elderly, trapped in their unheated homes. People tried to stay warm by burning charcoal indoors, causing an increase in carbon monoxide poisoning and house fires:

*At least a dozen houses...in Montgomery were damaged by fires caused by residents' efforts to stay warm or cook...after burning charcoal indoors. More than a hundred people spent Friday night in emergency shelters...Hospitals reported an influx of elderly in their emergency rooms.*<sup>37</sup>

In Maryland, the blackout moved Governor Parris Glendening to declare a state of emergency in six counties. The Governor activated the National Guard to assist firehouses.<sup>38</sup>

The power outage created a refugee population “of entire neighborhoods...searching for warmth and diversion at hotels, theaters, malls and even office towers.”<sup>39</sup> Thousands were “fleeing cold, dark homes,” according to press reports:

*Across the area, but especially in Montgomery, hotels filled to capacity with customers fleeing cold, dark homes. The 365-room Doubletree Hotel on Rockville Pike was sold out by 8 a.m.. Residence Inn by Marriott, on Wisconsin Avenue in Bethesda, with 187 rooms, was sold out by noon.*<sup>40</sup>

The blackout moved the **Washington Post** to observe that “daily life was crippled, if not halted—dramatically illustrating the fragile dependence of modern times on the flip of a switch.”<sup>41</sup>

### **The Great Ice Storm (January 1998)**

Starting on January 4<sup>th</sup> and for six days, until January 10, 1998, freezing rain fell across a 600-mile weather front that included parts of Ontario and Quebec in Canada, and Maine and upstate New York in the United States. Electric outages in the affected areas of Canada deprived 4.7 million people, or 16 percent of the Canadian population, of power, according to Emergency Preparedness Canada. In the United States, 546,000 people were without power (deprived of heat, light, and in many instances water) in the cold of mid-winter.<sup>42</sup>

---

<sup>36</sup> Scott Wilson, “Utilities Say Blackout Overwhelmed Medical Priorities,” **Washington Post** (22 January 1999), p. B3.

<sup>37</sup> Pan and Hsu, op. cit., p. A1.

<sup>38</sup> Ibid.

<sup>39</sup> Ibid.

<sup>40</sup> Ibid. Levine and Jackman, op. cit., p. A1.

<sup>41</sup> Levine and Jackman, op. cit., p. 1.

<sup>42</sup> Eugene L. Lecomte, Alan W. Pang, and James W. Russell, **Ice Storm '98** (Institute for Business and Home Safety: December 1998), pp. 1-2.

Some of the 5.2 million people affected by the Great Ice Storm of 1998 went without power for five weeks. It was the greatest natural disaster in Canadian history, and generated more insurance claims than Hurricane Andrew, the costliest natural disaster in U.S. history.<sup>43</sup>

One historian of the Great Ice Storm notes that “the storm’s biggest impact was, in a sense, not weather-related: It was the loss of electricity”:

*Ice accumulations caused the collapse of more than a thousand...transmission towers...More than 7,500 transformers stopped working....Some parts of Monteregie, a region of 1.3 million people southeast of Montreal, went without power for so long that the area became known as “the Dark Triangle.”*<sup>44</sup>

The blackout caused an immediate and life-threatening emergency in Montreal’s water supply that depended upon electricity for filtration and pumping. At 12:20 P.M. on January 9<sup>th</sup>, the two water filtration plants that served 1.5 million people in the Montreal region went down, leaving the area with only enough water to last 4 to 8 hours. Government officials kept the water crisis secret, fearing public knowledge would exacerbate the crisis by water hoarding. However:

*Even as officials deliberated, water pipes in some households were already dry. As reports and rumors of a water shortage spread, consumption jumped by 10 percent anyway, and bottled water disappeared from stores.*<sup>45</sup>

The **Toronto Star**, in an article entitled “Millions Shiver In Dark: How A Major City is Being Crippled by Deadly Ice Storm,” reported that parts of Montreal had run out of water, “and those who still had it were warned not to drink tap water without boiling it first.”<sup>46</sup> But most people had no way of boiling water.

Officials feared not only a shortage of drinking water, but an inadequate supply of water for fighting fires. So desperate was the situation that Alain Michaud, Fire Chief of Montreal, prepared to fight fires with a demolition crane instead of water, hoping that “if a building caught fire, it might burn to the ground, but the crane would demolish neighboring structures to prevent the fire’s spread.”<sup>47</sup> By 9:30 P.M. on January 9<sup>th</sup>, one of Montreal’s major reservoirs was nearly empty. Provincial officials considered evacuating the city. However, Hydro-Quebec, the government electric utility, managed to restore power to the filtration plants and restore water service.<sup>48</sup>

The blackout also threatened the food supply: “Food poisoning has become a real threat as embattled Montrealers, unable to get to stores, eat food that has been kept too long in

---

<sup>43</sup> Jacques Leslie, “Powerless,” **Wired** (April 1999), p.120.

<sup>44</sup> Ibid.

<sup>45</sup> Ibid, p. 176.

<sup>46</sup> Sandro Contenta, “Millions Shiver In Dark: How A Major City Is Being Crippled By Deadly Ice Storm,” **Toronto Star** (10 January 1998), p. A1.

<sup>47</sup> Leslie, op. cit., p. 176.

<sup>48</sup> Ibid.

refrigerators that don't work."<sup>49</sup> In upstate New York, the electric utility Niagara Mohawk announced that it was focusing restoration of electric power on more populated areas "so that supermarkets, gasoline stations and hotels could reopen, and people in the more rural areas could find food and shelter."<sup>50</sup> New York State Electric and Gas helped customers get to shelters and distributed 200,000 pounds of dry ice for storing food."<sup>51</sup> One typical resident of Canada's "Dark Triangle" complained, "I've lost all my food...I melt ice for water. It's no way for a family to live."<sup>52</sup>

Shelter, another basic necessity for survival, was also threatened by the mid-winter blackout: "People without power discovered just how many facets of their lives depended on electricity. Their stoves, appliances, and heating didn't work."<sup>53</sup> Many of Canada's newer, well-insulated homes relied on inexpensive electric heat.<sup>54</sup> Thousands of people fled their cold, dark homes to seek refuge in government and charitable shelters. The situation in Saint-Jean-sur-Richelieu, a working-class town of 36,000 was typical, where 3,600 people became shelter refugees, one-tenth of the population.<sup>55</sup> St. Hyacinthe in the "Dark Triangle" lost nearly half its residents, who mostly fled the city.<sup>56</sup> About 100,000 people took refuge in shelters.<sup>57</sup>

Communications, financial, and transportation infrastructures failed massively during the blackout. In upstate New York, only French Canadian radio stations were still on the air. In Ontario, 50,000 telephones went dead, frustrating the electric utility from restoring power service, since it relied on customer phone calls to locate power failures. Credit cards and ATM machines became useless, so all financial transactions had to be in cash.<sup>58</sup> The blackout shut down Montreal's four subway lines for the first time in the system's 30-year history.<sup>59</sup>

Underscoring that the blackout, not the ice storm, was the real crisis, the Canadian Premier Lucien Bouchard declared that "the most urgent need" was for generators, and appealed to anyone in Canada with a generator to help.<sup>60</sup> Bouchard also appealed to the U.S. Federal Emergency Management Agency, "asking for beds and generators to provide shelters with heat and light."<sup>61</sup>

Hospitals in Canada and the United States were nearly overwhelmed with blackout victims. In Maine, where six out of ten residents lost power, a single hospital, in Lewiston, reported

---

<sup>49</sup> Contenta, op. cit., p. A1.

<sup>50</sup> "Monster Ice Storm Slays Transmission Facilities In Quebec, Upstate New York," **Northeast Power Report** (McGraw-Hill: 16 January 1998), p. 1.

<sup>51</sup> "Canada And New England Still Reeling," **Electric Utility Week** (19 January 1998), p. 1.

<sup>52</sup> Jack Beaudoin, "Quebec In Crisis," **Portland Press Herald** (8 February 1998), p. 45.

<sup>53</sup> Leslie, op. cit., p. 176.

<sup>54</sup> Beaudoin, op. cit., p. 45.

<sup>55</sup> Leslie, op. cit., p. 178.

<sup>56</sup> Beaudoin, op. cit., p. 45.

<sup>57</sup> Leslie, op. cit., p. 122.

<sup>58</sup> Ibid, p. 176.

<sup>59</sup> Contenta, op. cit., p. A1.

<sup>60</sup> Mark Dunn, "Ice Storm Holds Eastern Ontario In Its Beautiful But Deadly Grip," **The Record** (9 January 1998), p. A1.

<sup>61</sup> Contenta, op. cit., p. A1.

treating for carbon monoxide poisoning 120 people “who ran generators, kerosene heaters and even charcoal grills in their homes to keep warm.”<sup>62</sup>

Hospital medical services underwent a crisis during the protracted blackout when their emergency generators failed. For example, at Montreal’s LeMoyne Hospital:

*The generators broke down on the sixth day, and the staff instantly switched to flashlights. For two hours until the generators were repaired, the hospital lost the use of its life-support and monitoring equipment: Nurses pumped air by hand into the lungs of patients on respirators and manually took each patient’s pulse and blood pressure every 15 minutes. Instead of one nurse for each six patients, a ratio of at least one-to-one was needed.*<sup>63</sup>

The blackout indirectly caused hundreds of deaths in Canada and the U.S., according to Great Ice Storm historian Jacques Leslie. Leslie criticizes the official death toll figures as too low:

*The official death toll was 45-28 fatalities in Canada, 17 in the U.S.—but those numbers understate the ice storm’s effects. Hundreds of ill and elderly people, weakened by extended stays in shelters where flu became epidemic, died weeks or months later, succumbing to ailments they might otherwise have overcome.*<sup>64</sup>

Over a year after the Great Ice Storm ended, according to Jaques Leslie, “The people who experienced it remain aware of one overriding lesson: Their dependence on electricity makes them more vulnerable than they’d ever imagined.”<sup>65</sup> Mark Abley, author of **The Ice Storm**, makes a similar observation:

*Huddling in school gyms, church halls, shopping malls, and other shelters, the evacuees didn’t pray for a return of fine weather. They prayed for a return of power. The ice storm demonstrated not that we are prisoners of brutal weather, but that we are all now hostages to electricity.*<sup>66</sup>

### **Western Heat Wave (10 August 1996)**

A heat wave, with near record high temperatures, blacked out large parts of nine western states on a torrid Saturday afternoon, August 10<sup>th</sup>, 1996. Near-record high temperatures covered most of the West at the time: for example, over 100 degrees in eastern Oregon and the San Joaquin Valley, 113 degrees in Red Bluff, and 104 degrees in Boise, Idaho.<sup>67</sup> Initial speculation that the blackout was sparked by a brushfire near Oregon was later discounted. According to

<sup>62</sup> Peter Pochna and Abby Zimet, “Facing Down An Ice Storm,” **Portland Press Herald** (18 January 1998), p. 1A.

<sup>63</sup> Leslie, op. cit., pp. 178, 180.

<sup>64</sup> Ibid, pp. 122-123.

<sup>65</sup> Ibid, p. 123.

<sup>66</sup> Ibid.

<sup>67</sup> Rich Connell, “Massive Power Outage Hits Seven Western States,” **Los Angeles Times** (11 August 1996), p. 1.

Dulcy Mahar, spokeswoman for the Bonneville Power Administration, the blackout was caused by the heat wave:

*Some of the lines sagged because of the heat. Some of those lines sagged down onto trees and then tripped off for safety reasons. The power that those lines were carrying was moved off to other lines and overloaded those, and then the safety devices tripped those lines off and you had the outages.*<sup>68</sup>

Although the blackout lasted less than 24 hours, it was “one of the largest power outages on record.”<sup>69</sup> The blackout affected “an estimated 4 million people in nine states, trapping people in elevators, snarling traffic and generally causing widespread chaos.”<sup>70</sup> The blackout caused problems that could have become a significant threat to life and society, had they been more protracted.

Water supplies were interrupted in some regions because electric pumps would not work. Arizona, New Mexico, Oregon, Nevada, Texas, and Idaho experienced blackout-induced disruption in water service during the heat wave. For example:

*In Fresno, where most of the city receives water from wells powered by electric pumps, the city manager declared a local emergency. Only two of the city’s 16 fire stations had water sources and most of the fire hydrants were out. The county and Air National Guard rushed in tankers to boost the Fire Department’s capacity.*<sup>71</sup>

Air and ground transportation systems experienced significant disruptions because of the blackout. For example, at San Francisco International Airport, although an emergency generator powered the control tower, other systems—security, computers, elevators, and luggage carousels—would not work. Jetways could not be positioned at airplane doors. An estimated 6,000 passengers were stranded.<sup>72</sup> Incoming flights had to be diverted to San Jose and Oakland. Airport Spokesman Bob Schneider announced, “We are pretty much out of business.”<sup>73</sup>

Signal lights failed, causing massive traffic jams in San Francisco and San Diego. “Traffic is a nightmare,” declared San Francisco Police Department spokesman Bruce Metdors, “They’re just backed up everywhere. It’s gridlock.”<sup>74</sup> San Francisco mass transit—electric trolleys and BART metro trains—were stalled by the blackout.<sup>75</sup> “We’re responding in what amounts to our earthquake mode,” said Orange County Fire Captain Dan Young, “We certainly had an increase

<sup>68</sup> Tim Golden, “Power Failure in 6 Weeks Creates Havoc for the West,” *New York Times* (12 August 1996), p. 13. See also Tina Griego, “Regulators Will Take Up Western Power Failures,” *Albuquerque Tribune* (12 August 1996), p. A1.

<sup>69</sup> Connell, op. cit., p. 1.

<sup>70</sup> Robert Dintleman, “Western Power Failures Traced To Soaring Temperatures,” *All Things Considered, National Public Radio* (11 August 1996), Transcript #2302-5.

<sup>71</sup> Connell, op. cit., p. 1.

<sup>72</sup> Ray Delgado, “Huge Blackout Hits West Coast,” *San Francisco Examiner* (11 August 1996), p. A1.

<sup>73</sup> Connell, op. cit., p. 1.

<sup>74</sup> Ibid.

<sup>75</sup> Delgado, op. cit., p. A1.

in traffic collisions, since you've got thousands of signals with no control on them.”<sup>76</sup> Gas pumps were out of order, stranding motorists who needed to refuel. “All the pumps run on electricity,” explained one station attendant, “When you think about it, everything runs on electricity.”<sup>77</sup>

“Even a few hours without electricity caused chaos,” according to press reports:

*Los Angeles police went on a citywide tactical alert as supervisors ordered some day shift officers to stay on duty into the night. Firefighters patrolled the city, responding to dozens of reports of stuck elevators. Department of Transportation crews checked on 4,000 intersections where the outage could have put traffic lights on the fritz. Blaring fire alarms and broken water lines added to the havoc.*<sup>78</sup>

Communications were disrupted by the blackout. “Radio stations reported power outages at locations throughout the midsection of California,” according to press reports, “In San Francisco, TV stations KPIX and KQED were off-line for some time due to the outage.”<sup>79</sup> Radio Station KNBR and the Canadian Broadcast Corporation went off the air.<sup>80</sup> Cable television networks crashed.<sup>81</sup>

Emergency medical services were disrupted by the blackout because “trauma rooms across the state [California] were cut off for hours from the radio that tells them an emergency is heading their way.”<sup>82</sup> Fire crews equipped with portable power generators were sent to doctors’ offices so the physicians could complete surgeries.<sup>83</sup> In Orange County, 200 fire units were dedicated to providing power to hospitals with emergency vehicles.<sup>84</sup>

The blackout disrupted control systems in some major industrial facilities. For example, the Chevron refinery in Richmond, California, “was unable to control flues due to the outage,” releasing “huge clouds of black smoke.”<sup>85</sup> The blackout caused power plants throughout the west—“including nuclear plants near Central California’s Morro Bay and west of Phoenix”—to shut down.<sup>86</sup> The Diablo Canyon nuclear power plant, near San Luis Obispo, shut down, and required several days for technicians to complete safety checks before it could be started again.<sup>87</sup>

<sup>76</sup> Kim Boatman and Lori Aratani, “Millions Lose Power,” **San Jose Mercury News** (11 August 1996), p. 1A.

<sup>77</sup> Marilyn Kalfus, Ana Menendez, and Julio Laboy, “Blackout Brings Much Of O.C. To A Halt,” **Orange County Register** (11 August 1996), p. A1.

<sup>78</sup> Connell, op. cit., p. 1.

<sup>79</sup> Delgado, op. cit., p. 1.

<sup>80</sup> Boatman and Aratani, op. cit., p. A1.

<sup>81</sup> Kalfus and et. al., op. cit., p. A1.

<sup>82</sup> Ibid.

<sup>83</sup> Douglas E. Beeman, “Hot West Goes Dim,” **The Press Enterprise** (11 August 1996), p. A1.

<sup>84</sup> Jim Hill, “West Coast Power Outage Easing In Some Locations,” **Show, CNN** (10 August 1996), Transcript #1600-4.

<sup>85</sup> Delgado, op. cit., p. 1.

<sup>86</sup> Beeman, op. cit., p. A1.

<sup>87</sup> Golden, op. cit., p. 13.



The Bonneville Power Administration told the press, “All of the utilities are relying on each other, and it has a cascading effect when one part experiences a major failure.”<sup>88</sup>

### **Hurricane Andrew (August 1992)**

Hurricane Andrew struck southern Florida on August 24, 1992 and reached the coast of Louisiana on August 26, two days later. Andrew has been described by some experts as the worst natural disaster in U.S. history.<sup>89</sup> Andrew laid waste to 165 square miles in South Florida, destroying some 100,000 homes in Florida and Louisiana, and leaving more than 3.3 million homes and businesses without electricity.<sup>90</sup>

Federal and state officials were at first unaware of the magnitude of the disaster and slow to react. Three days into the crisis, Kate Hale, the Director of Dade County’s Office of Emergency Management called a press conference to demand of state and federal authorities, “Where the hell is the cavalry on this one? We need food. We need water. We need people. For God’s sake, where are they?”<sup>91</sup>

By the end of the first week, President Bush had ordered 14,400 troops into the Florida disaster area “with mobile kitchens, tents, electrical generators, water and blankets....Even those lucky enough to have homes may not have electricity for more than a month.”<sup>92</sup>

Andrew’s aftermath posed an immediate threat to life in South Florida because of damage to the infrastructures for water and food. A widespread electrical blackout prevented pumps from working, so there was no running water.<sup>93</sup> Most grocery stores had been destroyed. Massive traffic jams, caused in part by non-functioning signal and street lights, prevented the surviving supermarkets from being re-supplied. To meet the crisis, the Army Corps of Engineers distributed more than 200,000 gallons of water and the Department of Agriculture gave out tons of surplus food.<sup>94</sup> Nonetheless, two weeks after the hurricane, food was still not reaching many victims. On September 7, fifteen days after Andrew struck, reporters witnessed the following scene:

*In the ruins, Charlie Myers, 65, stood holding a peach and a loaf of bread.  
“This is all I have left, he said. What plans did he have? “Survive buddy.”<sup>95</sup>*

Andrew’s blackout of the power grid made the crisis over water, food, and shelter worse by severing communications between relief workers and victims. Without power, there was an

---

<sup>88</sup> Delgado, op. cit., p. 1.

<sup>89</sup> “Mother Nature’s Angriest Child,” **Time** (7 September 1992), p. 15.

<sup>90</sup> Tom Mathews, Peter Katel, Todd Barrett, Douglas Waller, Clara Bingham, Melinda Liu, Steven Waldman, and Ginny Carrol, “What Went Wrong,” **Newsweek** (7 September 1992), p. 23.

<sup>91</sup> Ibid.

<sup>92</sup> “Mother Nature’s Angriest Child,” op. cit., p. 16.

<sup>93</sup> William Booth and Mary Jordan, “Hurricane Rips Miami Area, Aims at Gulf States,” **Washington Post** (25 August 1992), p. A7.

<sup>94</sup> Mathews and et. al., op. cit., p. 27.

<sup>95</sup> Ibid.

almost complete collapse of communications—no phones, radio or television.<sup>96</sup> “Without electricity to power radio and television sets, mass communication remains difficult or impossible,” according to authorities and press reports.<sup>97</sup> Consequently, people were unaware of relief efforts or of where to go for help. For example, although the U.S. Marines erected “tent cities” able to accommodate thousands of homeless hurricane victims, many did not know of this refuge: “Many people in the vast storm-stricken area, even those who live within easy walking distance of the sprawling encampment, said they were not aware of the tents’ existence.”<sup>98</sup> Unable to communicate where victims could get water, relief workers stacked “pyramids of bottled water...on street corners, free for the taking.”<sup>99</sup>

The blackout of power and communications, according to press reports, imbued “South Florida with an end-of-the world aura”:

*Hundreds of thousands of people found themselves in a Stone Age existence, left to pursue hunting and gathering, forced to forage for food and water. Because many people in the devastated areas had no radios or batteries, the location of food distribution sites has been a mystery....Each time word spread about establishment of a new relief outlet, people suddenly would swarm forward on foot, and National Guard troops often had to be summoned to keep order. The hurricane robbed steamy South Florida of the two amenities deemed essential to life here: air conditioning and ice cubes. “We can’t stand this heat any longer,” said Rita Larraz, whose house in South Dade County was spared but who, like 750,000 customers here, still had no electricity, and therefore no air conditioning in the 90-plus degree heat and humidity...”The heat is killing us.”<sup>100</sup>*

The blackout crippled the transportation infrastructure, further impeding relief efforts. “More than 5,000 traffic lights are on the blink...,” according to press reports. Consequently, “Traffic was snarled for miles. The simplest chore, indeed almost everything, seemed to take forever.”<sup>101</sup>

Andrew’s blackout of the power grid contributed significantly to societal anarchy in South Florida. With the blackout induced collapse of communications there was no way for survivors of Andrew to report crimes in progress. An orgy of looting provoked vigilantism. Unable to rely on the police, individuals armed themselves to protect their homes and remaining possessions.

<sup>96</sup> One report indicates the phone system continued to operate or experienced only partial failure. See John Mintz, “Phones Withstand Hurricane’s Fury,” **Washington Post** (26 August 1992), p. F1. For a different view see Booth and Jordan, op. cit. (25 August 1992), p. A7.

<sup>97</sup> Laurie Goodstein and William Booth, “Marines Ready Tent Cities in South Florida,” **Washington Post** (1 September 1992), p. A1.

<sup>98</sup> Ibid.

<sup>99</sup> Ibid.

<sup>100</sup> William Booth, “Hurricane’s Fury Left 165 Square Miles Pounded Into the Ground,” **Washington Post** (30 August 1992), p. A1.

<sup>101</sup> Goodstein and Booth, op. cit., p. A1.

“Andrew had made one zone of society come unglued,” according to **Newsweek**, “Disasters penetrate like lasers, revealing weaknesses beneath the smooth surfaces of a community.”<sup>102</sup> Lack of streetlights encouraged “thieves...to take advantage of a general feeling of lawlessness, particularly before federal troops began arriving”:

*At night, in darkened streets cordoned by National Guard troops enforcing a curfew, machine-gun fire has been heard. Spray-painted on the side of a house in Perrine was: “I’m armed and dangerous! Looters shot on sight!” “Everyone is armed, everyone is walking around with guns,” said Navy physician Sharon Wood, who worked at a mobile hospital in Homestead, where workers refused to dispense calming drugs such as valium for fear that word might get out and the hospital might be robbed. In Kendall, senior citizens sleep at night with revolvers by their sides....Miami and its surrounding municipalities, which have a long history of racial and ethnic tension, were considered a tinderbox.*<sup>103</sup>

Some 3,300 National Guard troops enforced a dusk-to-dawn curfew, when looting was worst, under cover of darkness. More than 200 people were arrested for looting or violating the curfew.<sup>104</sup> However, some efforts to restore law and order impeded relief efforts:

*Roadblocks set up to stop looters continued to hamper delivery of emergency food supplies. Truckers with emergency food aid were forced to wait for police escorts after reports that some drivers had been shot and beaten by thugs. State troopers thwarted the progress of some private help when they began stopping all trucks entering the state, demanding that the drivers show that they and their cargo had been officially requested and that they were from a recognizable organization.*<sup>105</sup>

Ultimately, some 16,000 federal troops from every branch of the armed forces turned the lights back on and restored order to South Florida.<sup>106</sup>

---

<sup>102</sup> Mathews and et. al., op. cit., p. 24.

<sup>103</sup> Booth, op. cit., p. A18.

<sup>104</sup> William Booth and Mary Jordan, “Painful Awakening in South Florida,” **Washington Post** (26 August 1992), p. A27.

<sup>105</sup> Mary Jordan, “President Orders Military to Aid Florida,” **Washington Post** (28 August 1992), p. A14.

<sup>106</sup> Rick Gore, “Andrew Aftermath,” **National Geographic** (April 1993), p. 20.

VOLUME II

# **Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures**

**JULY 2017**

**Report of the Commission to Assess the Threat to the United States  
from Electromagnetic Pulse (EMP) Attack**



# Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures

**July 2017**

REPORT OF THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES  
FROM ELECTROMAGNETIC PULSE (EMP) ATTACK

---



The cover photo depicts Fishbowl Starfish Prime at 0 to 15 seconds from Maui Station in July 1962, courtesy of Los Alamos National Laboratory.

This report is a product of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. The Commission was established by Congress in the FY2001 National Defense Authorization Act, Title XIV, and was continued per the FY2016 National Defense Authorization Act, Section 1089.

The Commission completed its information-gathering in June 2017. The report was cleared for open publication by the DoD Office of Prepublication and Security Review on April 9, 2018.

This report is unclassified and cleared for public release.

TABLE OF CONTENTS

---

EXECUTIVE SUMMARY ..... 1

1 INTRODUCTION ..... 2

2 GROUND CONDUCTIVITY PROFILES ..... 7

3 SOVIET E3 HEMP MEASUREMENTS ..... 9

    Test Parameters..... 9

    Scaling of the Results..... 19

    Latitude Scaling..... 19

    Pattern Scaling..... 20

4 CONCLUSIONS..... 24

## LIST OF FIGURES

---

Figure 1	Parts of HEMP. E3 HEMP heave is roughly described by the second peak in the MHD signal. [SOURCE: Meta R-321] .....	3
Figure 2	Diagram of the E3 HEMP heave effect. [SOURCE: Meta R-321] .....	4
Figure 3	Sample normalized yield variation for maximum E field for heave for burst heights between 130 and 170 km and for a fixed Earth conductivity profile. [SOURCE: Meta R-321].....	5
Figure 4	Sample normalized HOB variation for maximum peak E field for heave for an intermediate yield weapon and for a fixed Earth conductivity profile. [SOURCE: Meta R-321].....	6
Figure 5	Ground conductivity depth profile for three ground profiles. ....	7
Figure 6	Ground profile B-to-E conversion in the frequency domain for three cases. ....	8
Figure 7	Simulation of the Soviet tests showing B field peaks and field directions, 150 km test (R2). ....	10
Figure 8	Simulation of the Soviet tests showing B field peaks and field directions, 300 km test (R1). ....	11
Figure 9	Measured B fields at N1, 150 km test.....	12
Figure 10	Measured B fields at N2, 150 km test.....	12
Figure 11	Measured B fields at N3, 150 km test.....	13
Figure 12	Measured B fields at N1, 300 km test.....	13
Figure 13	Measured B fields at N2, 300 km test.....	14
Figure 14	Measured B fields at N3, 300 km test.....	14
Figure 15	E field amplitudes for four ground profiles, at N1, 150 km test.....	16
Figure 16	E field amplitudes for four ground profiles, at N2, 150 km test.....	16
Figure 17	E field amplitudes for four ground profiles, at N3, 150 km test.....	17
Figure 18	E field amplitudes for four ground profiles, at N1, 300 km test.....	17
Figure 19	E field amplitudes for four ground profiles, at N2, 300 km test.....	18
Figure 20	E field amplitudes for four ground profiles, at N3, 300 km test.....	18
Figure 21	Geomagnetic latitude variation, for a 150 km burst, over the U.S. The black line is at 48.92°, which is the computed geomagnetic latitude for the 150 km Soviet test.....	20
Figure 22	Normalized simulated B field peaks versus ground range for the 150 km test. The black dot shows the simulated results for the N3 point.....	21
Figure 23	Normalized simulated B field peaks versus ground range for the 300 km test. The black dot shows the simulated results for the N3 point.....	22
Figure 24	E field waveform shape, using the measured N1 waveform from the 150 km burst height .....	24
Figure 25	Normalized E peak contour pattern from the 150 km burst case .....	25

LIST OF TABLES

---

Table 1    Geometry for the Soviet High-Altitude Tests. ....9

Table 2    Peaks of the Soviet measurement waveforms. (The E field is for the 10<sup>-3</sup> S/m  
ground.) ..... 15

Table 3    Geomagnetic latitude scaling of the Soviet measurements. ....21

Table 4    Pattern (observer position) scaling of the Soviet measurements.....22

Table 5    Scaling of the Soviet Measurements.....24

## ACRONYMS AND ABBREVIATIONS

---

B	magnetic field
CONUS	continental United States
DoD	Department of Defense
E	electric field
EMP	electromagnetic pulse
EPRI	Electric Power Research Institute
FERC	Federal Energy Regulatory Commission
GMD	geomagnetic disturbance
HEMP	high-altitude electromagnetic pulse
HOB	height of burst
km	kilometer
m	meter
MHD	magnetohydrodynamic
min	minute
NERC	North American Electric Reliability Corporation
nT	nanotesla
S/m	siemens/m
UV	ultraviolet
V	Volt

## PREFACE

---

This EMP Commission Report, utilizing unclassified data from Soviet-era nuclear tests, establishes that recent estimates by the Electric Power Research Institute (EPRI) and others that the low-frequency component of nuclear high-altitude EMP (E3 HEMP) are too low by at least a factor of 3. Moreover, this assessment disproves another claim--often made by the U.S. Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), EPRI and others—that the FERC-NERC Standard for solar storm protection against geo-magnetic disturbances (8 volts/kilometer, V/km) will also protect against nuclear E3 HEMP. A realistic unclassified peak level for E3 HEMP would be 85 V/km for CONUS as described in this report. New studies by EPRI and others are unnecessary since the Department of Defense has invested decades producing accurate assessments of the EMP threat environment and of technologies and techniques for cost-effective protection against EMP. The best solution is for DoD to share this information with industry to support near-term protection of electric grids and other national critical infrastructures that are vital both for DoD to perform its missions and for the survival of the American people.



## EXECUTIVE SUMMARY

---

As described in this report, there is a need to have bounding information for the late-time (E3) high-altitude electromagnetic pulse (HEMP) threat waveform and a ground pattern to study the impact of these types of electromagnetic fields on long lines associated with the critical infrastructures. It is important that this waveform be readily available and useful for those working in the commercial sectors.

While the military has developed worst-case HEMP waveforms (E1, E2, and E3) for its purposes, these are not available for commercial use. Therefore, in this report openly available E3 HEMP measurements are evaluated from two high-altitude nuclear tests performed by the Soviet Union in 1962. Using these data waveforms and an understanding of the scaling relationships for the E3 HEMP heave phenomenon, bounding waveforms for commercial applications were developed.

Since the measured quantities during these tests were the magnetic fields, it is possible to compute the electric fields assuming ground conductivity profiles that produce significant levels. There are other profiles that would compute even higher electric fields, but some of these profiles do not cover a very large area of the Earth.

After computing the electric fields using the Soviet measurements, the results were scaled to account for the fact that their measurement locations were not at the optimum points on the ground to capture the maximum peak fields. Through this process, it was determined that the scaled maximum peak E3 HEMP heave field would have been 66 volts per kilometer (V/km) for the magnetic latitude of the Soviet tests.

As the E3 HEMP heave field also increases for burst points closer to the geomagnetic equator, the measured results were also evaluated for this parameter. This scaling increases the maximum peak electric field up to 85 V/km for locations in the southern part of the continental U.S., and 102 V/km for locations nearer to the geomagnetic equator, as in Hawaii. The levels in Alaska would be lower at an estimated peak value of 38 V/km (see Table 5 for information dealing with this scaling process).

It is noted that this report does not claim that the values provided here are absolute worst-case field levels, but rather these peak levels are estimated based directly on measurements made during Soviet high-altitude nuclear testing.

## 1 INTRODUCTION

---

Over many years beginning in the 1980s, the U.S. has worked to establish the peak field levels, ground patterns of the heave portion of the late-time E3 HEMP fields as shown in Figure 1, and from these to build useful models.<sup>1,2</sup> In the summer of 1994, Soviet scientists attending the European Electromagnetics (EUROEM) Symposium in Bordeaux, France, presented several papers indicating their understanding of the different types of EMP including the high-altitude electromagnetic pulse (HEMP). One of the most interesting developments of that conference was that these presentations summarized the Soviet high-altitude electromagnetic test results and indicated that the most important aspects of the effects they observed were caused by the “long tail” of the HEMP.<sup>3</sup> In later publications, they indicated that the long tail referred to the late-time HEMP, or the E3 HEMP magnetohydrodynamic (MHD)-EMP heave signal, and later provided detailed technical information indicating that the failure of one long-haul communications line was due to this portion of the HEMP.<sup>4</sup> Three other references dealing with E3 HEMP (MHD-EMP) were published by Soviet scientists in this time frame presumably due to their interest in understanding the failures of commercial long line systems during their 1962 high-altitude nuclear testing program over Kazakhstan.<sup>5,6,7</sup>

Later in the early 2000s, Soviet scientists provided the EMP Commission with a memo that illustrated their magnetic field measurements of the E3 HEMP heave signals at three locations during two of their high-altitude nuclear tests over Kazakhstan in 1962.<sup>8</sup> Because the Soviets tested over land instead of over ocean, as did the U.S., several long line systems were affected by the E3 HEMP fields. In addition, measurements of the magnetic fields were made at several locations on the ground at various ranges from the surface zero (the point directly underneath the high-altitude burst).

- 
- <sup>1</sup> J. Gilbert, J. Kappenman, W. Radasky and E. Savage, “The Late-Time (E3) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid,” Meta R-321, January 2010.
  - <sup>2</sup> J.L. Gilbert, W.A. Radasky, K.S. Smith, K. Mallen, M.L. Sloan, J.R. Thompson, C.S. Kueny and E. Savage, “HEMPTAPS/HEMP-PC Audit Report,” Meta R-131, December 1999; DTRA-TR-00-1, April 2002.
  - <sup>3</sup> V.M. Loborev, “Up to Date State of the NEMP Problems and Topical Research Directions,” Proceedings of the European Electromagnetics International Symposium -- EUROEM 94, June 1994, pp. 15-21.
  - <sup>4</sup> V.N. Greetsai, A.H. Kozlovsky, V.M. Kuvshinnikov, V.M. Loborev, Y.V. Parfenov, O.A. Tarasov and L.N. Zdoukhov, “Response of Long Lines to Nuclear High-Altitude Nuclear Pulse (HEMP),” IEEE Transactions on EMC, Vol. 40, Issue 4, 1998, pp. 348-354.
  - <sup>5</sup> V.N. Greetsai, V.M. Kondratiev, and E.L. Stupitsky, “Numerical Modelling of the Processes of High-Altitude Nuclear Explosion MDH-EMP Formation and Propagation,” Roma International Symposium on EMC, September 1996, pp. 769-771.
  - <sup>6</sup> “The Physics of Nuclear Explosions,” Ministry of Defense of the Russian Federation, Central Institute of Physics and Technology, Volumes 1 and 2, ISBN 5-02-015124-6, 1997. MHD-EMP topics are found in Sections 13.5 and 13.6.3.
  - <sup>7</sup> V.M. Kondratiev and V.V. Sokovikh, “Redetermination of MHD-EMP Amplitude Characteristics and Spatial Distribution on the Ground Surface,” Roma International Symposium on EMC, September 1998, pp. 129-132.
  - <sup>8</sup> “Characteristics of magnetic signals detected on the ground during the Soviet nuclear high-altitude explosions,” memorandum provided by Soviet scientists, February 2003.

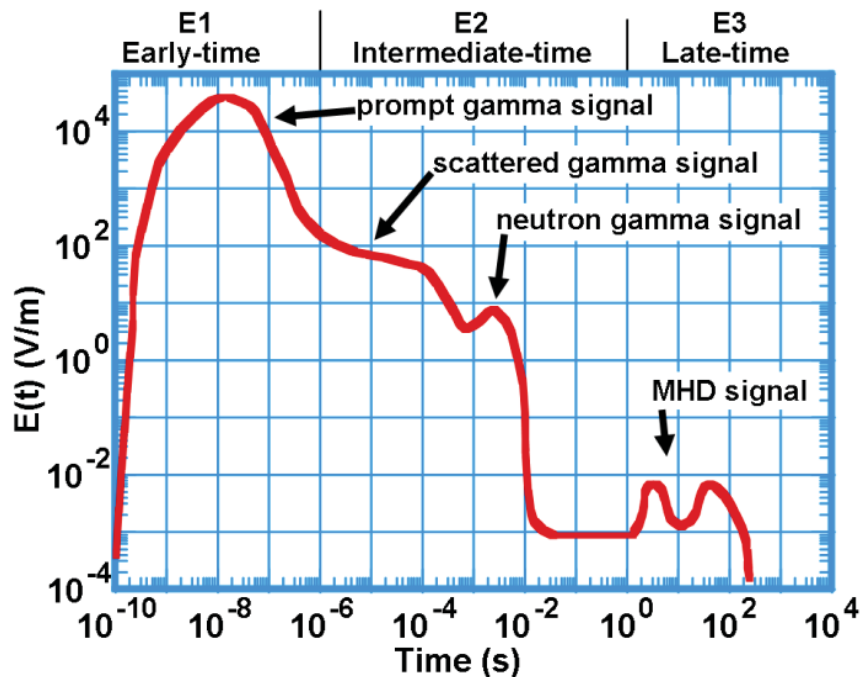


Figure 1 Parts of HEMP. E3 HEMP heave is roughly described by the second peak in the MHD signal. [SOURCE: Meta R-321]

In this report, the Soviet magnetic field data is reviewed, and through the use of several different ground conductivity profiles for locations in the U.S., the electric fields at the Earth's surface that could be induced are calculated. The magnetic fields are created by the nuclear detonation and the electric fields are induced in the earth and vary due to the particular deep conductivity profiles in the Earth. In addition, the magnetic fields (and electric fields) were also scaled to account for the fact that the Soviet measurements were not at the optimum ground locations to obtain the maximum peak fields on the ground. Finally, the increases in peak fields that would occur due to the well understood scaling of E3 HEMP with magnetic latitude were estimated, as the latitude of the Soviet tests were not at the bounding locations on the Earth.

The objective of this report is to determine from open source information how high the electric fields could be at latitudes of interest for the United States. In addition, a ground pattern and typical normalized electric field waveform is estimated that could be used for studies to determine the levels of quasi-DC currents that could be induced in long-line systems such as the bulk power system.

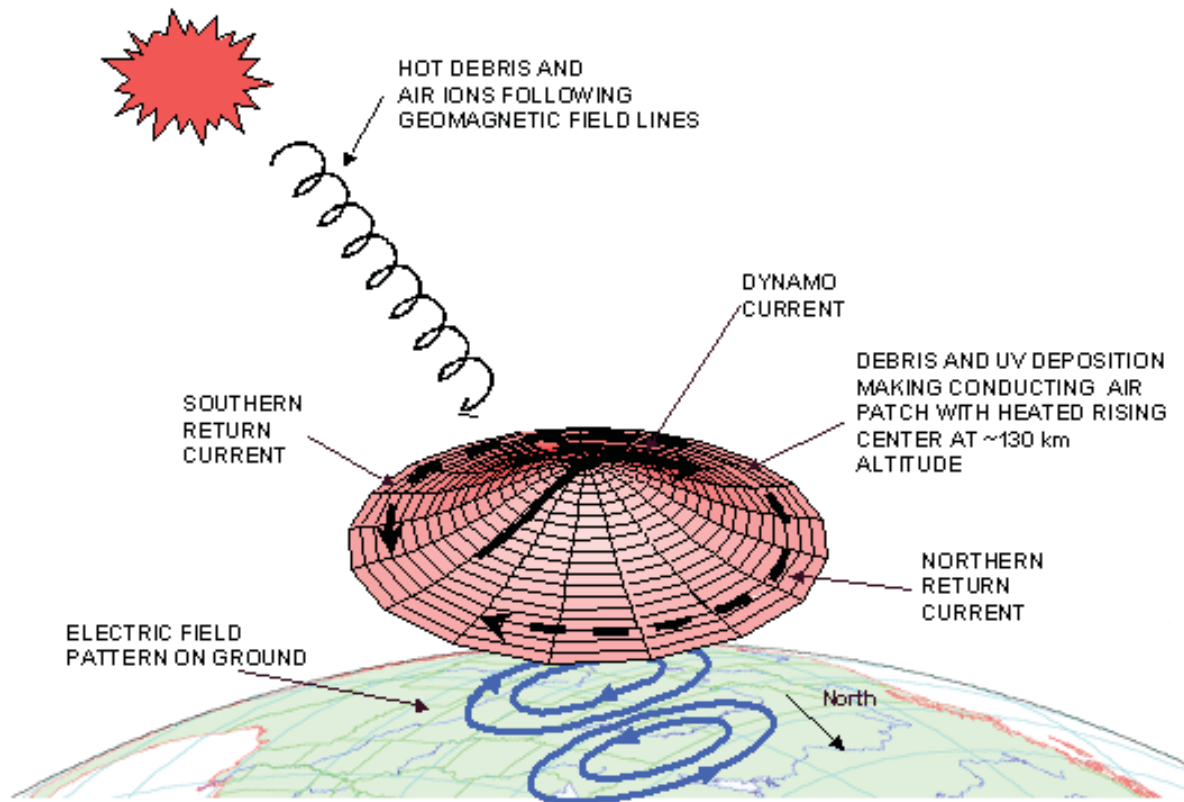
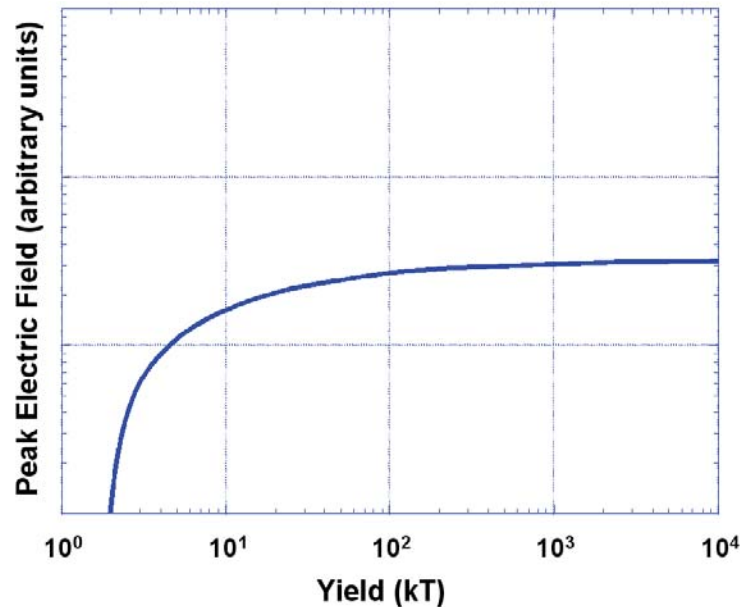


Figure 2 Diagram of the E3 HEMP heave effect. [SOURCE: Meta R-321]

This report does not claim that the values suggested here are absolute worst-case field levels, but rather these peak levels are estimated based directly on measurements made during high-altitude nuclear testing.

Figure 2 represents the E3 HEMP heave generation process. Hot ionized debris streaming downward away from the burst is directed preferentially along the geomagnetic field lines. As the debris and ultraviolet (UV) radiation from the burst reach altitudes where the atmosphere becomes dense enough, they heat up a “patch” of the atmosphere, and also add ionization to the background ionization already present in the ionosphere. The heat causes expansion, and the ionized region rises due to buoyancy. The Lorentz force on the ions and free electrons moving upward in the Earth’s geomagnetic field leads to east-west dynamo currents, with return currents completing the current flow on the north and south side. These currents induce image currents, with the associated electric fields, in the conductivity of the Earth below. Associated with this are magnetic (B) fields. The levels of the generated E fields are dependent on the actual ground conductivity to great depths of the Earth below the heaving patch, while the associated B field perturbations are approximately independent of the ground profile. For



*Figure 3 Sample normalized yield variation for maximum E field for heave for burst heights between 130 and 170 km and for a fixed Earth conductivity profile. [SOURCE: Meta R-321].*

this reason, the measured B fields on the Earth's surface can be considered to be the principal E3 HEMP heave environment.

It is noted that there is a second mechanism that creates E3 HEMP fields on the ground called "Blast Wave", but while it also can produce significant B fields, the maximum fields are found thousands of kilometers away from ground zero. For this reason, the Blast Wave phenomenon is not considered in this report.

The E3 HEMP heave B field perturbation on the ground depends on many parameters, such as:

1. Burst parameters: The characteristics of the burst are important. Of primary importance is the burst yield—bigger bombs would tend to have more debris coming down and generating the E3 HEMP heave signal. Figure 3 shows a sample of E3 HEMP heave variation with yield. This yield dependence can vary with the burst height. In addition, the area of coverage for the peak field tends to be larger for larger yields.
2. Burst location: The burst location has two important effects. First, the height of burst (HOB) is important for E3 HEMP heave, as it is for other HEMP phenomena. The precise interaction with the atmosphere depends on how high the burst is above the atmosphere. Also, the higher the burst, the farther north (for northern hemisphere bursts) the heated patch is found, as it needs to travel a further distance on the tilted

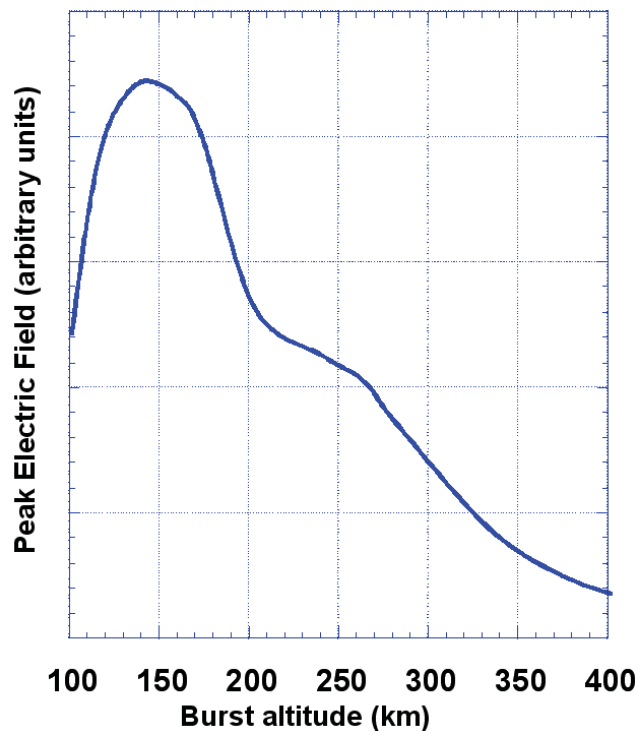


Figure 4 Sample normalized HOB variation for maximum peak E field for heave for an intermediate yield weapon and for a fixed Earth conductivity profile. [SOURCE: Meta R-321].

geomagnetic field lines. Figure 4 shows a sample of HOB variation for a fixed yield and ground conductivity profile. The other important location effect is the local geomagnetic field, which is represented by the value of geomagnetic latitude. One effect is that E3 HEMP heave gets weaker as the burst gets closer toward the (geomagnetic) poles, because the geomagnetic field becomes less horizontal, and there is less east-west deflection of the rising hot ions. (The geomagnetic latitude also affects the tilt of the path that the debris follows downward from the burst.)

3. Observer location: As seen in Figure 2, there is a 2-loop pattern of ground fields. The magnitude of the ground fields decreases with distance from the point directly below the patch. Examples of ground patterns are provided later in this report.
4. Burst time of day: Here the important factor is the “atmosphere”, basically the state of the ionosphere, which can vary significantly. Depending on the burst time, the day of the year, and the location, the burst may be in “night” or “day”. Sun exposure enhances the ionization of the ionosphere. For the E3 HEMP Blast Wave (the early-time portion of the E3 HEMP, which is not the subject of this report) the enhancement due to the “daytime” conditions depresses the E3 HEMP Blast Wave field, while for E3 HEMP heave there is an enhancement of the fields.



## 2 GROUND CONDUCTIVITY PROFILES

The E3 HEMP signal of concern in this report is the induced horizontal electric (E) field, as this field can effectively couple to long power and communications lines and induce quasi-dc currents in these systems. This coupling process has been discussed in several references including one that deals with geomagnetic disturbances (GMDs); GMD electric fields are similar in their time and frequency content to the electric fields produced by the E3 HEMP heave.<sup>9</sup> These E fields are produced by the presence of the conductivity depth profile in the Earth itself. For E3 HEMP heave it is the conductivity down to great depths (400-700 km) below the Earth's surface that determines the electric field. The E3 HEMP generation process begins with magnetic field (B) perturbations (relative to the geomagnetic field created by the Earth's core), and at the Earth's surface these B fields are little affected by the ground conductivity profile. Thus both calculations and measurements for actual nuclear tests typically begin with the B fields, and then E fields can be calculated for any assumed ground conductivity profile. While the induced peak E field is strongly related to the time derivative (dB/dt) of the horizontal B field, these calculations use the full Maxwell's Equations to determine the electric fields. The resulting E field is also horizontally oriented. The calculation of E from B must be done in terms of vector components—a B field in one horizontal direction creates an E field that is perpendicular to it under an assumed one-dimensional approximation for the local Earth conductivity profile.

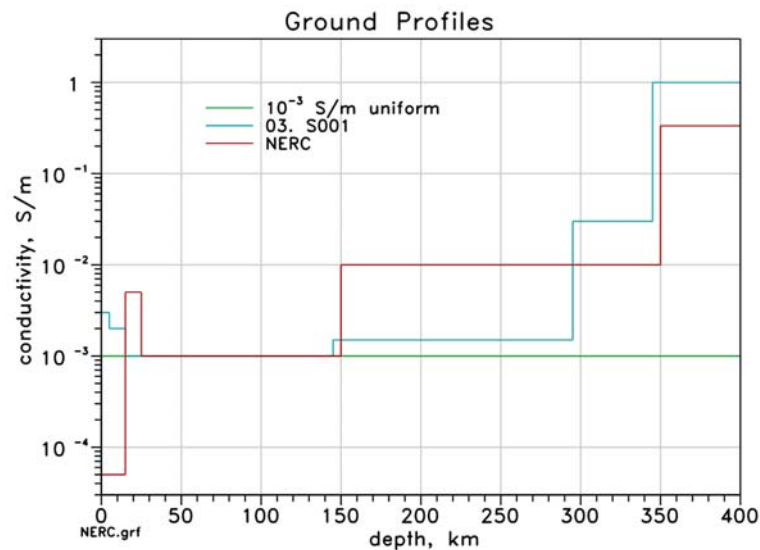


Figure 5 Ground conductivity depth profile for three ground profiles.

Figure 5 shows three ground profiles of ground conductivity with depth used in this report. The NERC profile (red line) has four layers of various conductivity levels, ending at a high

<sup>9</sup> W.A. Radasky, "Overview of the Impact of Intense Geomagnetic Storms on the U.S. High Voltage Power Grid," IEEE Electromagnetic Compatibility Symposium, Long Beach, California, 15-19 August 2011, pp. 300-305.

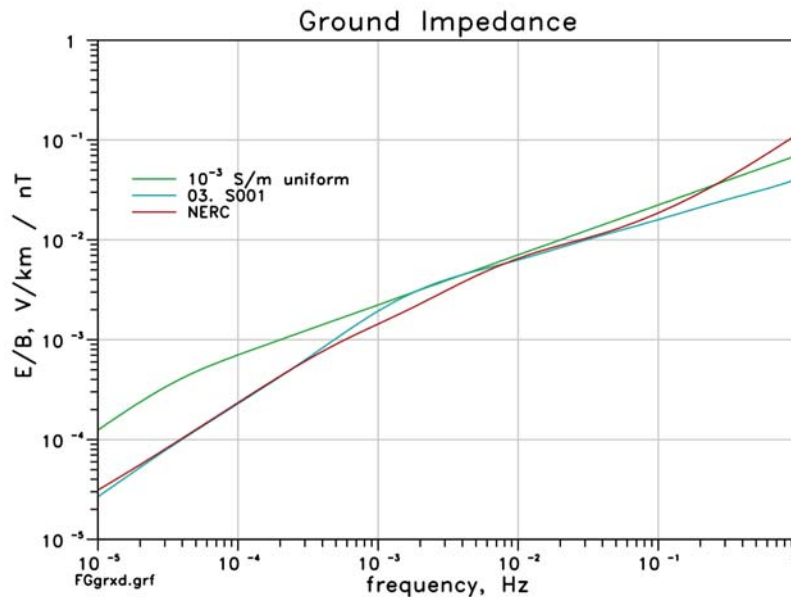


Figure 6 Ground profile B-to-E conversion in the frequency domain for three cases.

conductivity level that continues downward at its last value.<sup>10</sup> The E3 HEMP heave signals (due to their low frequency content) can penetrate through the upper layers of the Earth but will not penetrate much deeper when they encounter a high conductivity lower level (due to the pressures and temperatures found in the upper mantle of the Earth). The blue line is another set of ground conductivity data applicable to eastern Canada developed by Metatech from geological data. The impedance curve developed from this conductivity profile is seen to be very similar to the NERC curve in Figure 6. The third profile shown (in green) has a uniform conductivity of  $10^{-3}$  S/m, which is used for simplicity in the E3 HEMP heave simulations shown later in this report.

Figure 6 shows the resulting impedance (conversion of B to E) in the frequency domain. There are many ways to deal with these types of impedance curves relating E to B, although the technique used by the authors allows calculations of E from B in the time domain without converting to the frequency domain.<sup>11</sup> This has advantages for performing real-time computations when measuring geomagnetic storm disturbances. All three curves are reasonably close together for the important frequency range of 1 to 100 mHz, as this is the frequency range of typical E3 HEMP B-field disturbances.

<sup>10</sup> "Transmission System Planned Performance for Geomagnetic Disturbance Events", TPL-007-1, available at <https://bit.ly/2GQpQF1>

<sup>11</sup> J.L. Gilbert, W.A. Radasky and E.B. Savage, "A Technique for Calculating the Currents Induced by Geomagnetic Storms on Large High Voltage Power Grids," IEEE EMC Symposium, Pittsburgh, August 2012, pp. 323-328.

### 3 SOVIET E3 HEMP MEASUREMENTS

Toward the end of the development of the E3 HEMP computational models in the U.S., a paper that reported measurements made by the Soviet Union during two of their high-altitude nuclear tests in 1962 was provided to us through the U.S. Congressional EMP Commission by Soviet scientists.<sup>12</sup> This was high quality data, in that measurements were made at three fixed locations (designated N1, N2, and N3 by the Soviets as shown in Table 1 and Figure 7), and the B field measurements were provided for two horizontal vector components. There is some uncertainty concerning the precision of the test and measurement locations; however, the data provided greatly increased the information describing the E3 HEMP heave signal. High-altitude nuclear tests were performed by the U.S. mainly over the Pacific Ocean, and the locations for measuring the magnetic fields were not as diverse as for the Soviet measurements.

#### TEST PARAMETERS

The Soviet tests were reported to be at burst heights of 150 and 300 km altitudes, for the same device design with an estimated yield of 300 kT. The precise geometry (burst and observer locations) is not known, as there was some ambiguity in the data provided. The Soviet measurement paper does give range values (burst to observer distances) for all six measurements (three from each test), and these same values appear elsewhere in a consistent manner. (The Soviets tended to use the slant range from the burst to the ground location, not the ground range, but the ground range is easily calculated from the burst height.) A set of locations was used that are consistent with these values in the following discussions, using the understanding of the variation of the fields with location. These burst and observer locations are given in Table 1.

*Table 1 Geometry for the Soviet High-Altitude Tests.*

Test Locations			
Type	Position	Latitude (N)	Longitude (E)
Bursts	R1, 300 km	47.6°	64.9°
	R2, 150 km	47.0°	68.0°
Observers	N1	47.9°	67.4°
	N2	47.1°	70.6°
	N3	45.9°	72.1°

<sup>12</sup> "Characteristics of magnetic signals detected on the ground during the Soviet nuclear high-altitude explosions," memorandum provided by Soviet scientists, February 2003.

Using the simulation code in Meta R-321, the B field peak values were calculated for the two burst heights. The data is shown in Figure 7 for the 150 km burst height (R1) and in Figure 8 for 300 km (R2).<sup>13</sup> (The 300 km test was actually performed 6 days before the 150 km test, but the lower altitude case was described first). The peak contours are identified by their color, and the B field directions at the time of the peak are shown by the arrows. The burst and observer points are marked on the displays. Normalized results are shown in these figures as a nominal contour plot is desired to be used later in this report as a standard contour profile.

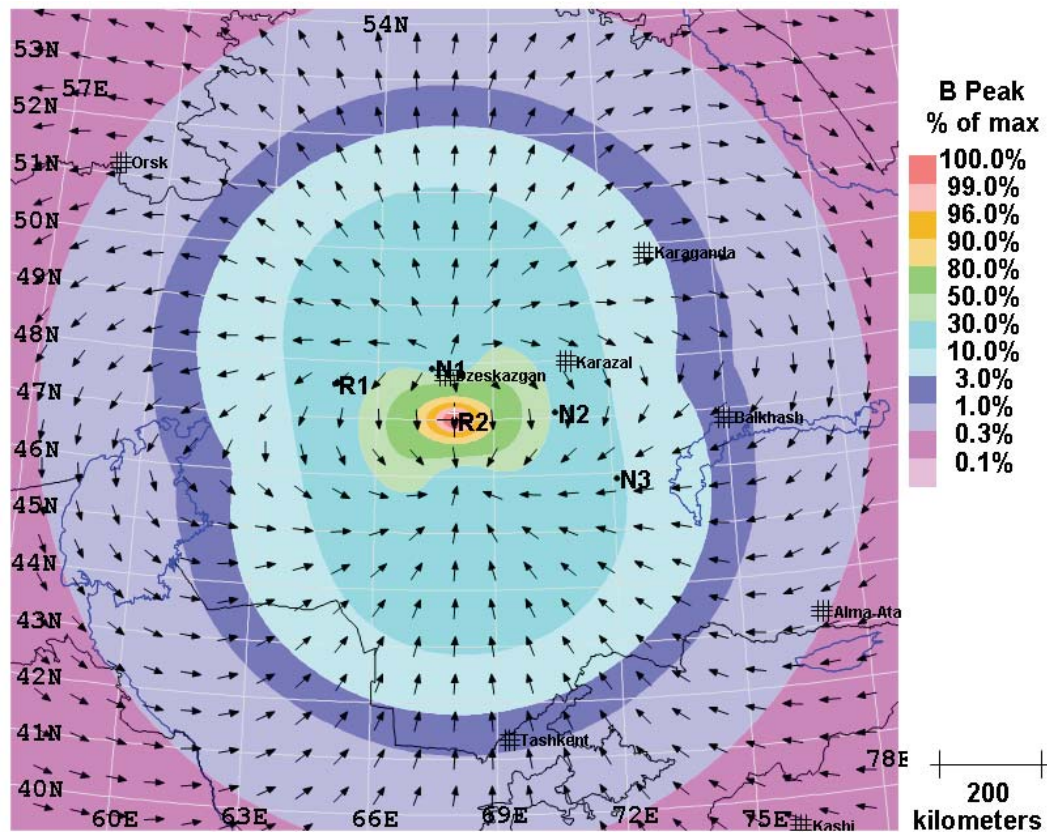


Figure 7 Simulation of the Soviet tests showing B field peaks and field directions, 150 km test (R2).

<sup>13</sup> J.L. Gilbert, W.A. Radasky, K.S. Smith, K. Mallen, M.L. Sloan, J.R. Thompson, C.S. Kueny and E. Savage, "HEMPTAPS/HEMP-PC Audit Report." Meta R-131, December 1999; DTRA-TR-00-1, April 2002.



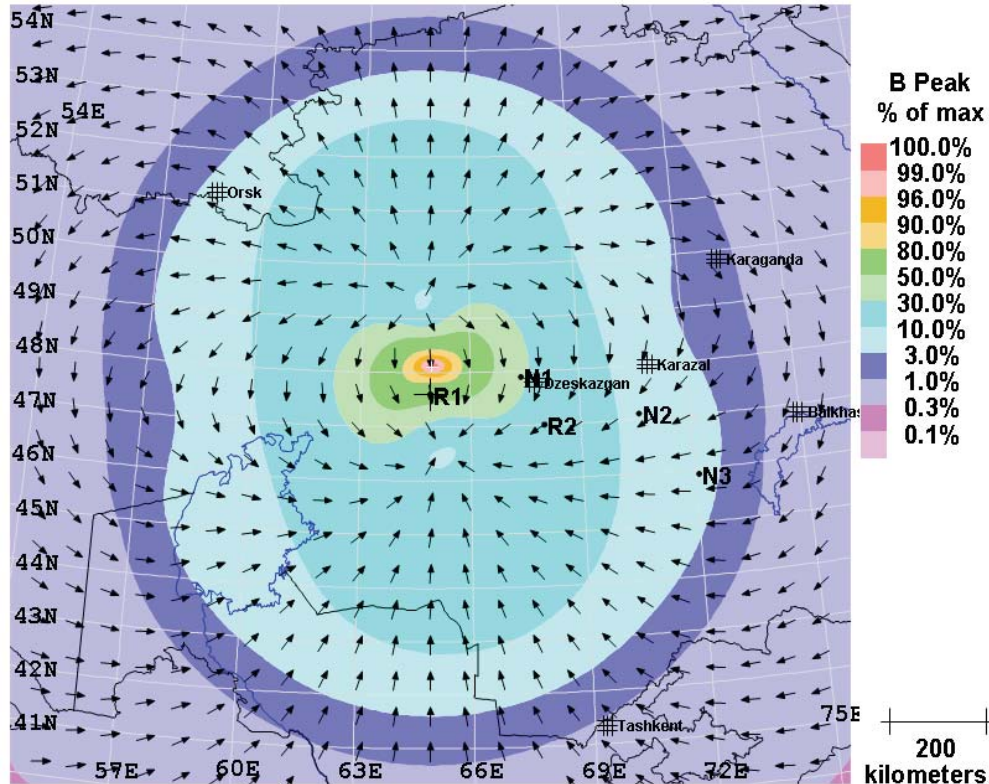


Figure 8 Simulation of the Soviet tests showing B field peaks and field directions, 300 km test (R1).

The next set of figures shows the measured B field time waveforms. The three lines are the north and west components, and the resulting magnitude. For the 150 km burst height case, shown in Figure 9 to Figure 11, the waveforms are all relatively wide in pulse width (the N1 case waveform has not returned to zero at the end of the 100-second window of the measurements). The peak occurs between times of 35 to 70 seconds. Figure 7 shows that N1 is close to the northern area of the two electric field depression points (the locations around which the two loops of E field circulate, as seen earlier in Figure 2) for this case. Here the time waveform may be complicated due to some shifting with time of the field depression point position. For the 300 km burst height waveforms, Figure 12 to Figure 14, the signals are faster, especially for N1. As noted, faster rising waveforms for the B fields enhance the E fields, because the impedance of the Earth behaves as  $f^{1/2}$  ( $f$  = frequency) as shown in Figure 6.

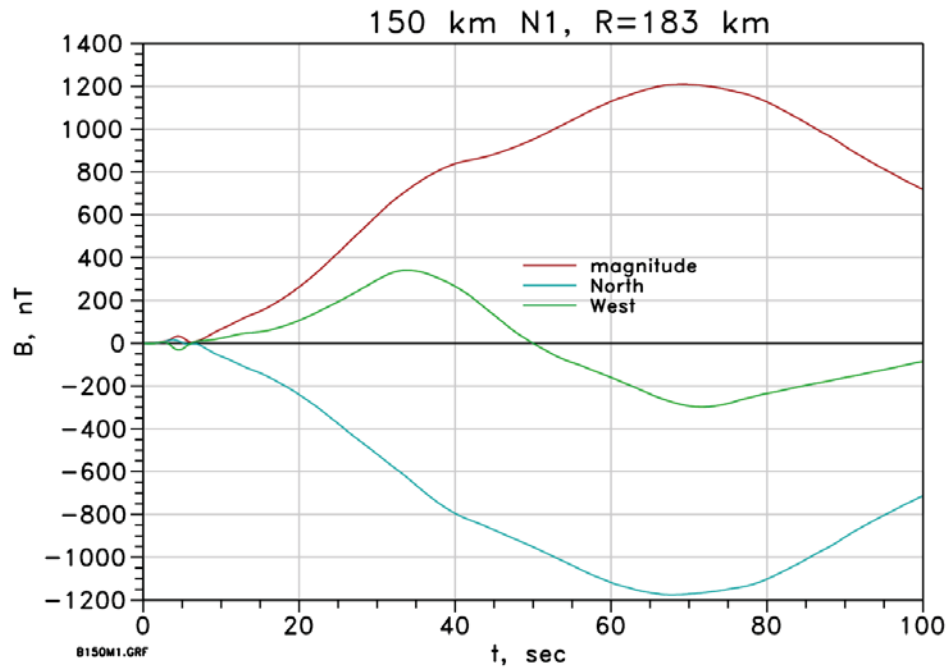


Figure 9 Measured B fields at N1, 150 km test.

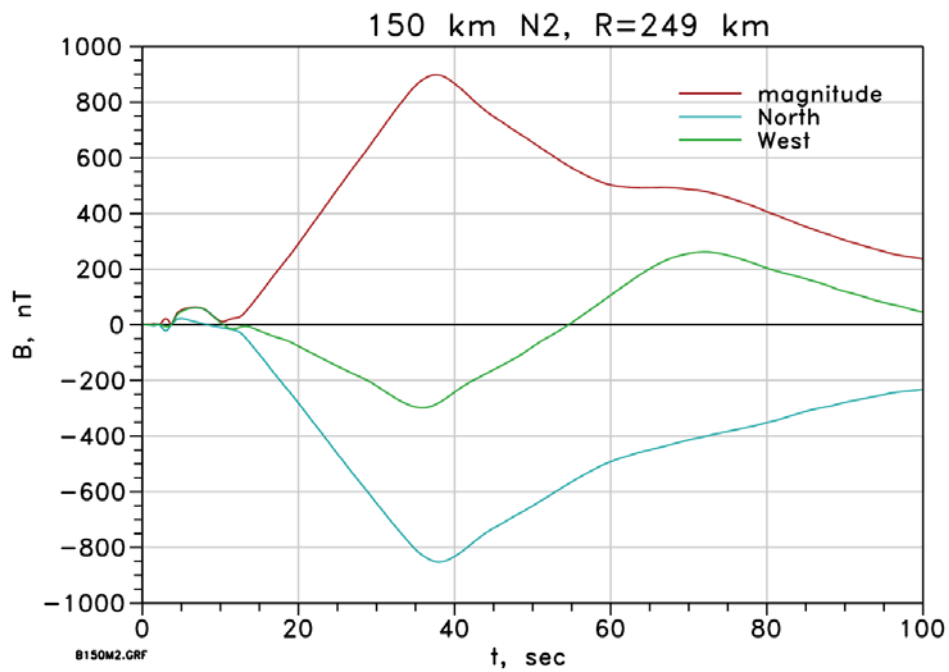


Figure 10 Measured B fields at N2, 150 km test.



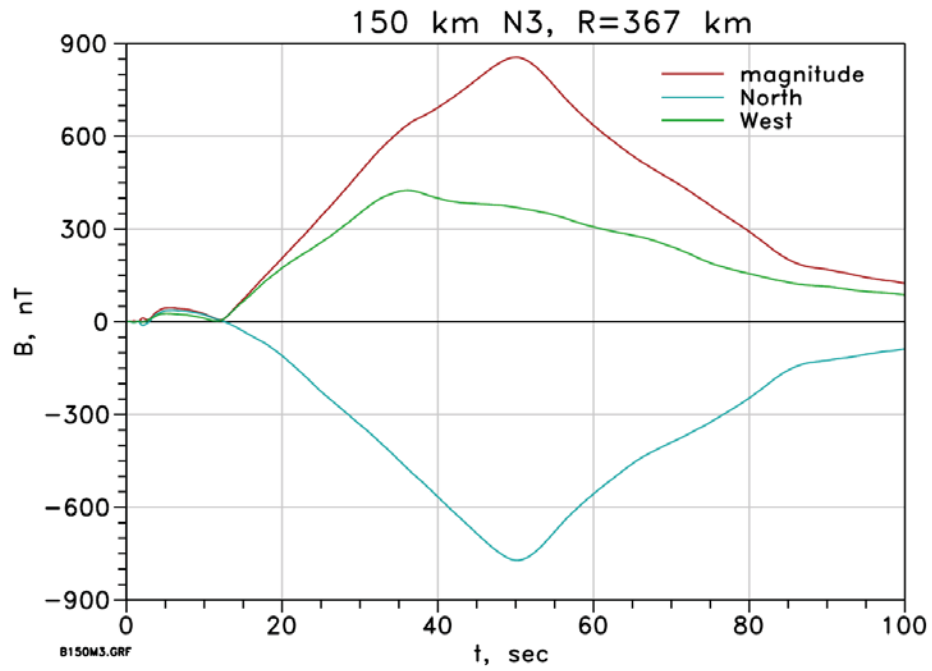


Figure 11 Measured B fields at N3, 150 km test.

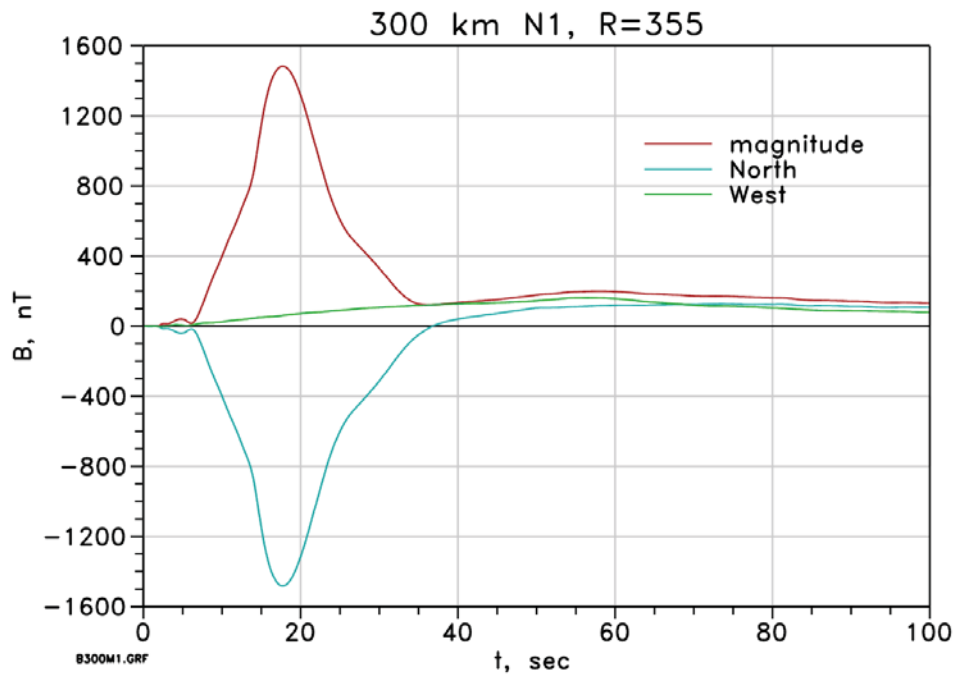


Figure 12 Measured B fields at N1, 300 km test.

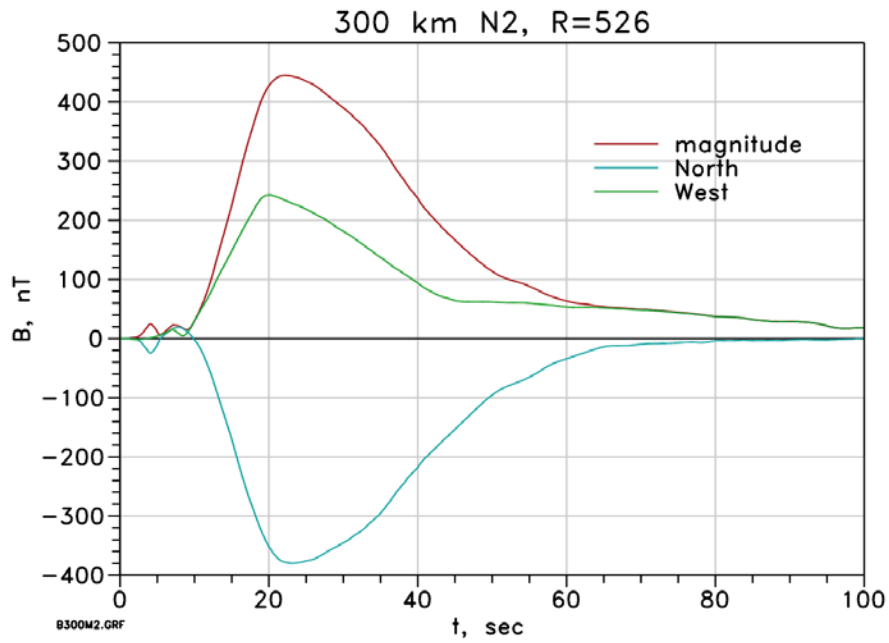


Figure 13 Measured B fields at N2, 300 km test.

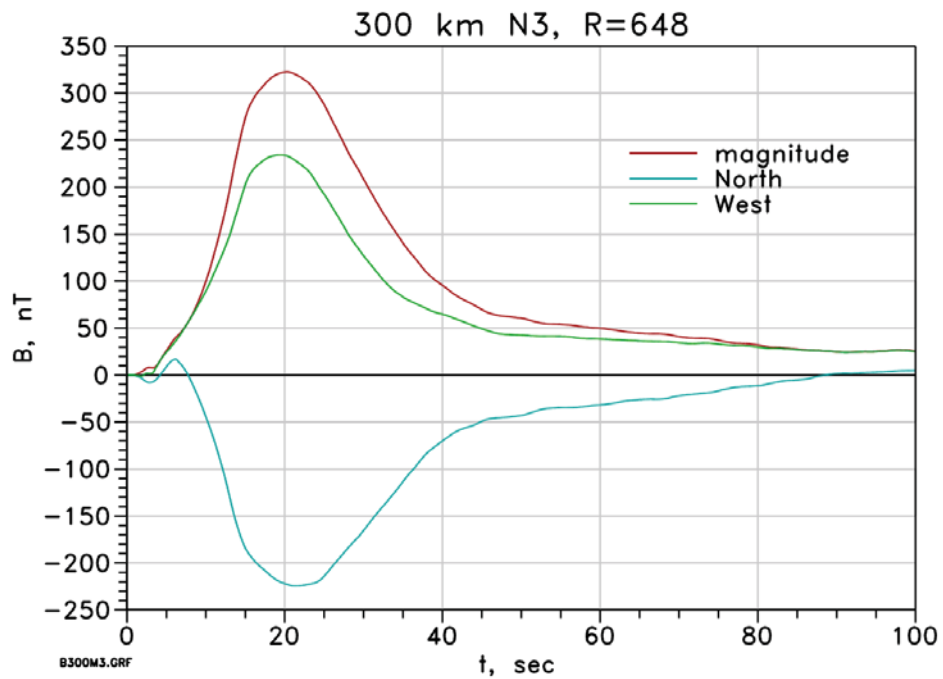


Figure 14 Measured B fields at N3, 300 km test.

The electric fields are now calculated from the measured B fields, given in nanoTeslas (nT). Table 2 lists the peak values for the calculated E fields, along with the peak values for the measured B and B-dot. The time derivative of B is often a good proxy for the behavior of the peak value of the electric field for a given ground conductivity profile. That is to say that for a given profile increases in the time derivative of the B field result in higher peak electric fields. It is noted, however, that the rest of the computed time waveform of the electric field depends more on the shape of the impedance curve and using the time derivative of the B field to compute the entire electric field waveform will not result in an accurate E field waveform.

For the following plots the measured B field components were individually computed for four sample ground profiles (a fourth severe ground profile and impedance curve was added to the previous set of three), and the resulting E field magnitudes are plotted (the total horizontal electric field is calculated by separately calculating the electric fields from the two orthogonal B field components). The 150 km cases are presented in Figure 15 to Figure 17, and the 300 km cases are presented in Figure 18 to Figure 20. These show that E fields are similar for the three ground profiles described in Figure 6. Further, the dark blue line shows the E field for a ground profile that has a very low conductivity. This profile was developed for southern Sweden and has also been used for a limited region in the northeastern United States, but it has not been used to develop the E3 HEMP results here. It is presented only to indicate that large electric fields are possible in some locations.

The highest computed E fields are for the N1 observer for the 300 km burst case. This had the highest measured B fields, and also had the narrowest time waveform—the computed peak E fields are driven higher by the enhanced time derivative of the B.

*Table 2 Peaks of the Soviet measurement waveforms. (The E field is for the  $10^{-3}$  S/m ground.)*

Measurement Peaks				
Burst	Observer	Peaks		
		B, nT	$\dot{B}$ , nT/min	E, V/km
R2 150 km	N1	1208.99	2141.2	4.885
	N2	898.27	3526.3	5.580
	N3	856.08	2240.2	4.241
R1 300 km	N1	1484.05	17581.4	16.585
	N2	444.69	3064.8	4.110
	N3	322.57	2642.9	3.113

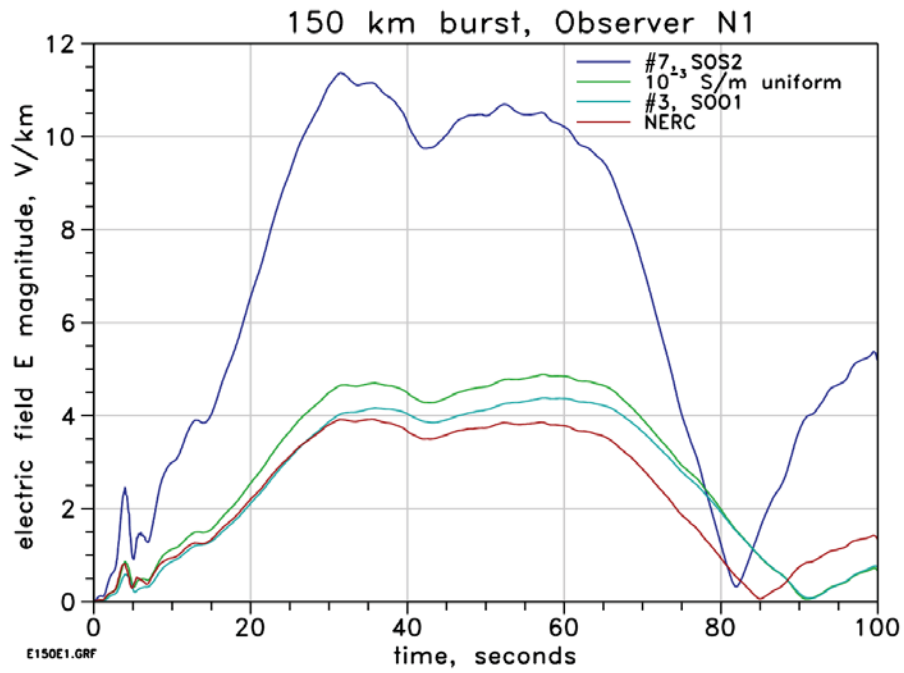


Figure 15 E field amplitudes for four ground profiles, at N1, 150 km test.

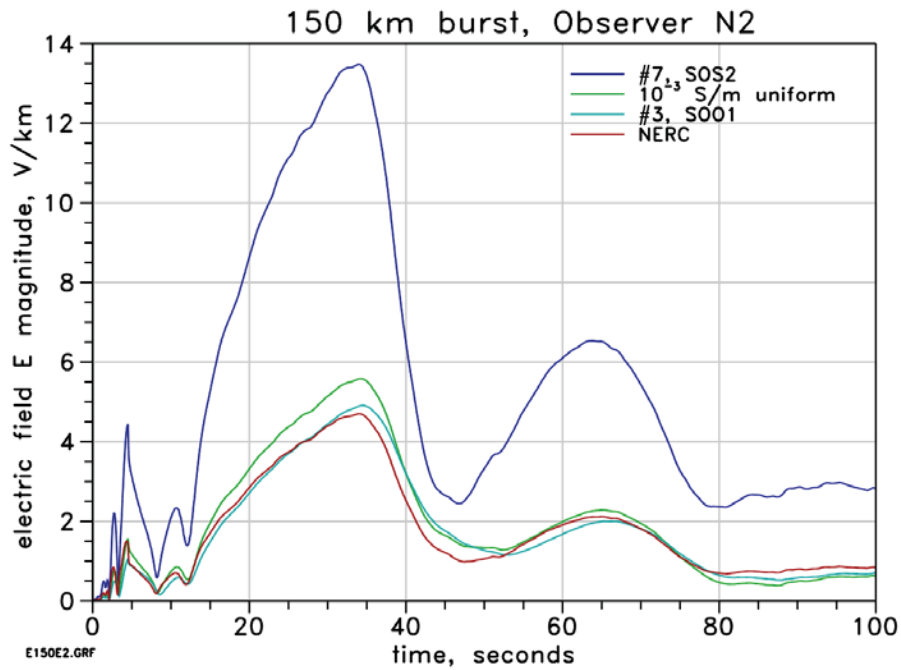


Figure 16 E field amplitudes for four ground profiles, at N2, 150 km test.

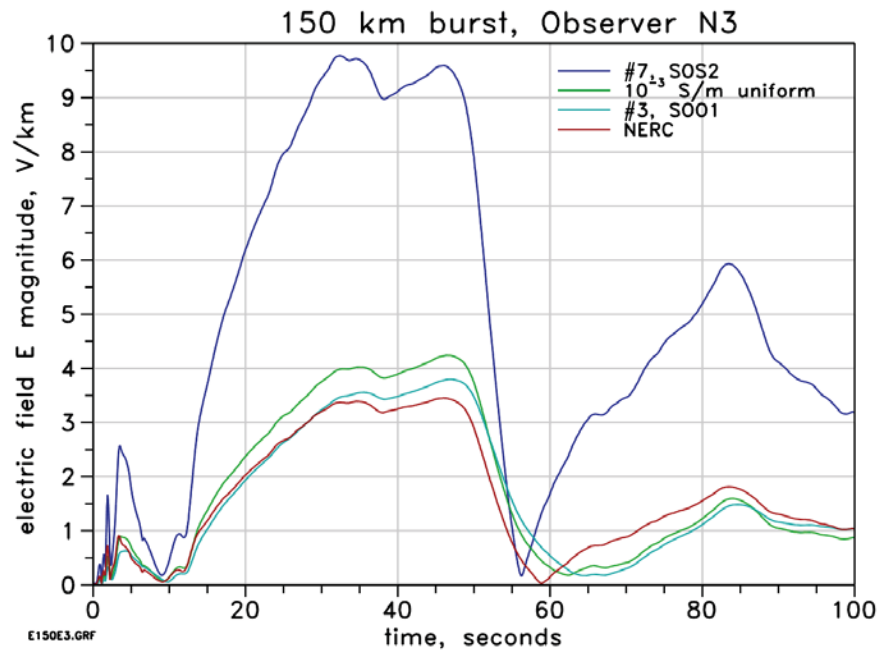


Figure 17 E field amplitudes for four ground profiles, at N3, 150 km test.

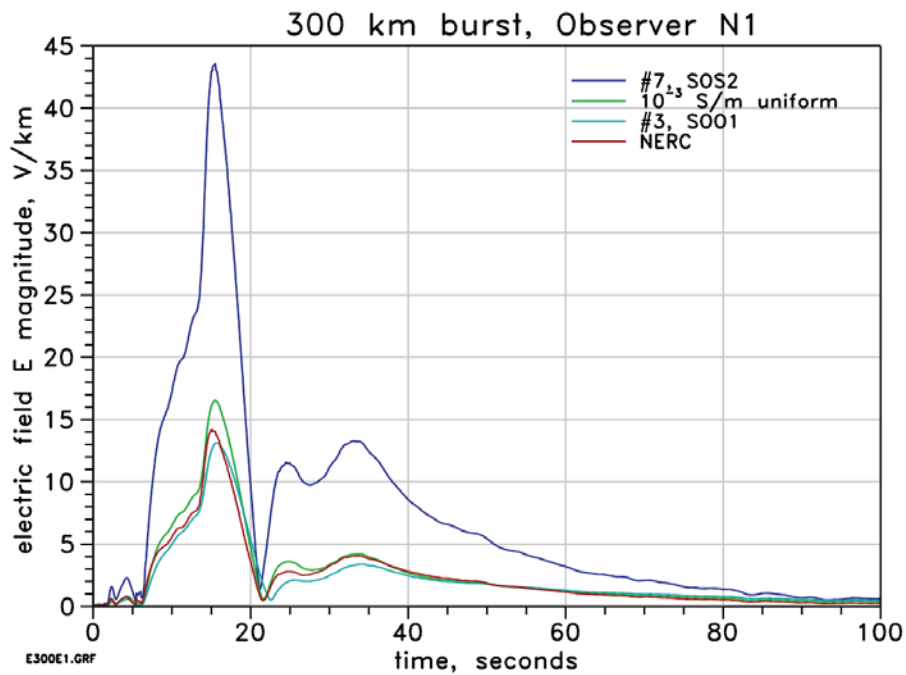


Figure 18 E field amplitudes for four ground profiles, at N1, 300 km test.

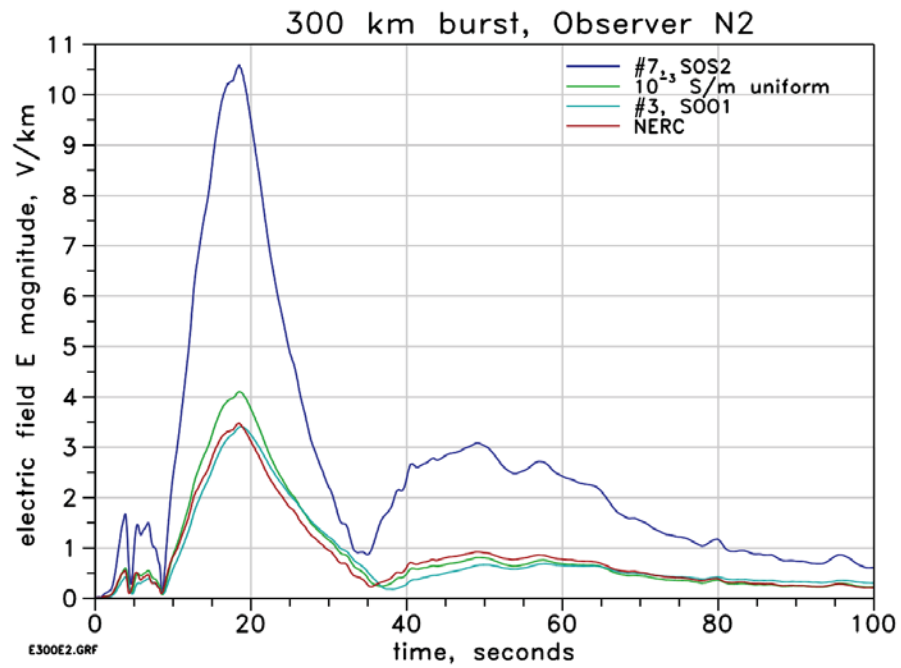


Figure 19 E field amplitudes for four ground profiles, at N2, 300 km test.

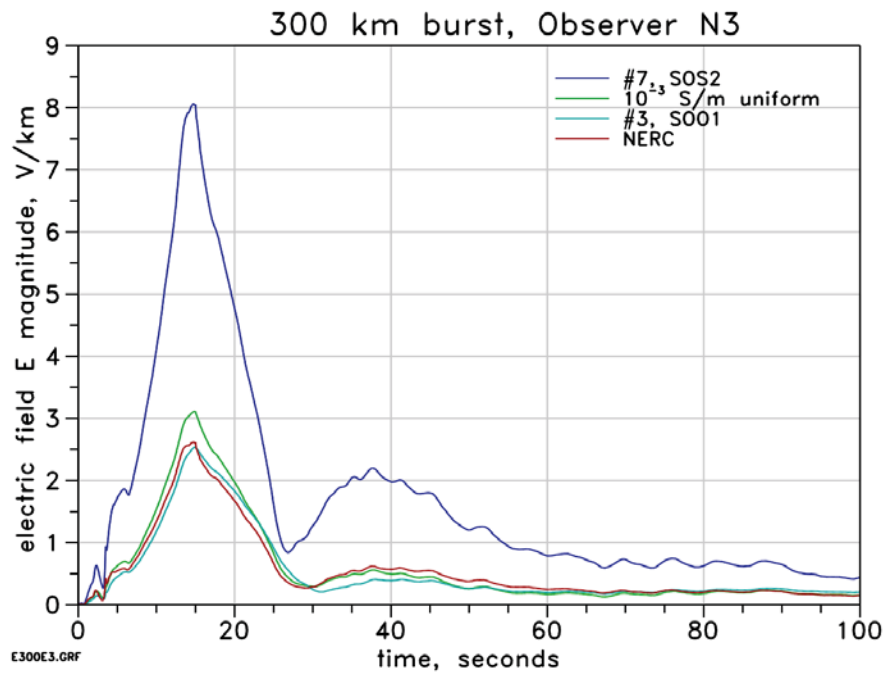


Figure 20 E field amplitudes for four ground profiles, at N3, 300 km test.



## SCALING OF THE RESULTS

Even at this date the calculational models of E3 HEMP heave are not considered to be perfect, and therefore measurements are the most believable evidence of possible E3 HEMP heave field levels. However, it is extremely unlikely that even these few high-quality measurements captured the highest peak fields. Of course other test devices, especially with higher yields, could have produced higher fields, and there can be vast variations in the atmosphere conditions. For this report, the parameters of interest are the locations of the measurement observers and of the burst itself. Specific parameters are the impacts due to the geomagnetic latitude of the bursts, and whether a better location exists to place measurement sites relative to each burst. The first question is: how much higher could the measured fields have been if the burst location were closer to the geomagnetic equator? The second question is because the fields were measured at only three locations, none of which were likely to have been at the optimum point, can the measurements be scaled to the optimum point?

## LATITUDE SCALING

The first consideration is the geomagnetic latitude. The geomagnetic latitude values for the two cases are found from the given physical locations:

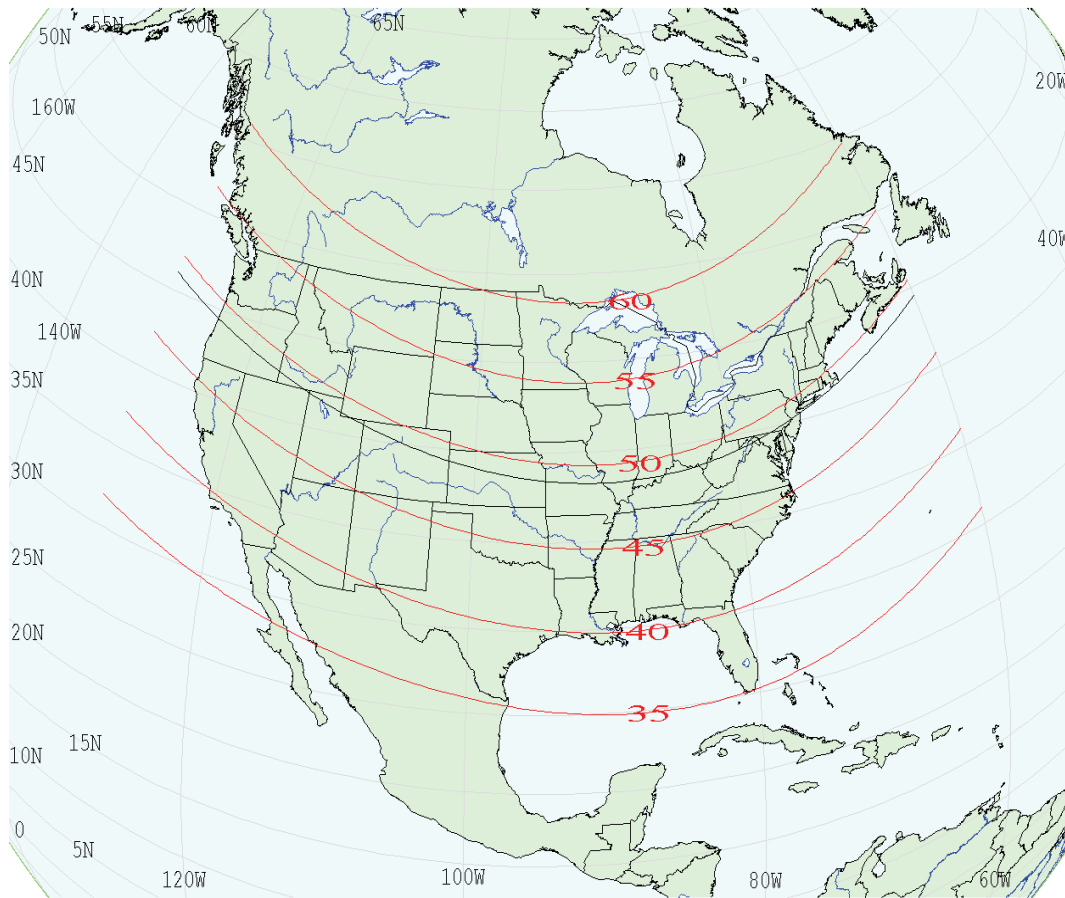
150 km: 48.92° N

300 km: 46.13° N

These values depend on knowing the burst locations, for which there is some uncertainty, but the precise values were likely within a few degrees of these values. As discussed, the maximum peak magnetic fields increase for lower geomagnetic latitudes per the basic models.

Considering the 150 km burst case, Figure 21 shows the equivalent locations for the continental U.S. The marked red lines show geomagnetic latitude lines, and there is a black line for the 48.92°N magnetic latitude corresponding to the 150 km HOB Soviet test. If the burst had been placed anywhere along this line, the maximum peak B fields would have been as in the Soviet test. For bursts below (south) this black line, the fields would be higher.

The map shows that Texas and Florida can be as low as 35°N geomagnetic latitude. The simulation code used to perform the calculations was the same as used for the simulations shown in Figure 7 and Figure 8, but with the burst moved to lower geomagnetic latitudes—specifically the cases of 35°N that correspond to the southern points for Florida and Texas, and also for the highest levels worldwide (the geomagnetic equator). Next, the ratios of the maximum B fields from these simulations at other latitudes were compared to the maximum values for the Soviet measurement location, to get the results shown in Table 3. Using these ratio values, the Soviet measurements (“Soviet” column) were scaled to the corresponding maxima for the other latitude burst locations.



*Figure 21 Geomagnetic latitude variation, for a 150 km burst, over the U.S. The black line is at 48.92°, which is the computed geomagnetic latitude for the 150 km Soviet test.*

Locations outside of the continental U.S. include both lower and higher geomagnetic latitudes. The table therefore includes scaling for a magnetic latitude of 22° N, which is appropriate for Oahu, Hawaii, and also for a magnetic latitude of 65° N, as would apply to Fort Greely, Alaska.

## PATTERN SCALING

The burst locations were different for the two tests, but the three observer locations stayed the same for the two tests. There is some uncertainty, however, in both the burst points and observer points. However, it is likely that the fields were higher at locations other than the three places that happened to be selected for the measurement sites. Here some understanding is sought for how high the measured fields might have been if there was a measurement at the optimal location. Figure 7 (the 150 km case), for example, shows that for this HOB the maximum is close to being directly under the burst, but the measurement sites were further out.

Table 3 Geomagnetic latitude scaling of the Soviet measurements.

Scaling of Measurements to Other Magnetic Latitudes								
Burst (km)	Observer	Burst Locations						
		Soviet, B, nT	Alaska, 65° N		U.S., 35° N		Hawaii, 22° N	
			Scaling factor	B, nT	Scaling factor	B, nT	Scaling factor	B, nT
R2 150	N1	1208.99	0.600	725.28	1.364	1648.65	1.675	2025.50
	N2	898.27		538.88		1224.93		1504.93
	N3	856.08		513.56		1167.40		1434.24
R1 300	N1	1484.05	0.577	855.62	1.274	1890.47	1.537	2280.36
	N2	444.69		256.38		566.47		683.29
	N3	322.57		185.98		410.91		495.66

As noted, there is some uncertainty in the modeling and for the model parameters to use to simulate the Soviet tests. Good confidence exists, however, in the values for the ranges to the measurement sites. With this in mind, the simulation shown in Figure 22 performs E3 HEMP heave calculations at points on a 2D polar mesh; for each range of this mesh all the azimuth angles were searched to obtain three norm values: maximum, average, and minimum. The overall maximum was identified and the three norm values were normalized to this maximum value, to obtain the three lines in the plot.

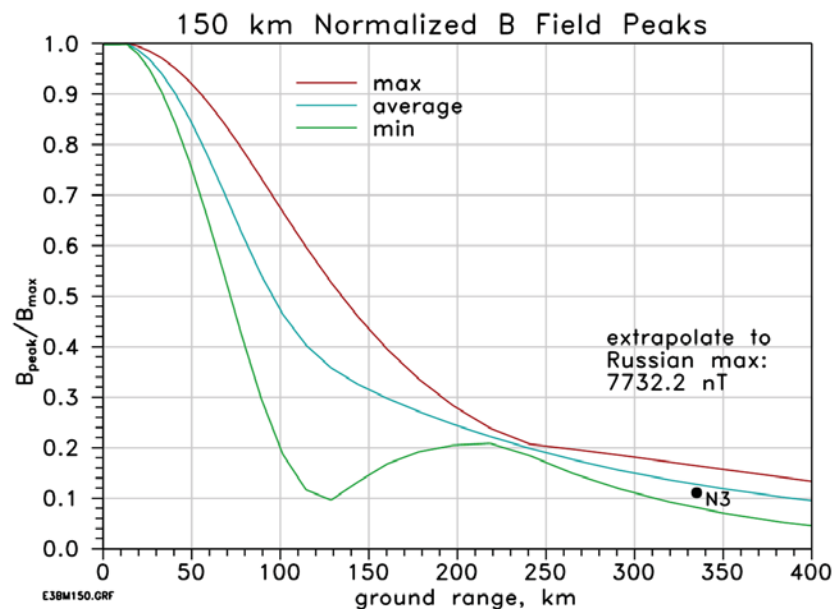


Figure 22 Normalized simulated B field peaks versus ground range for the 150 km test. The black dot

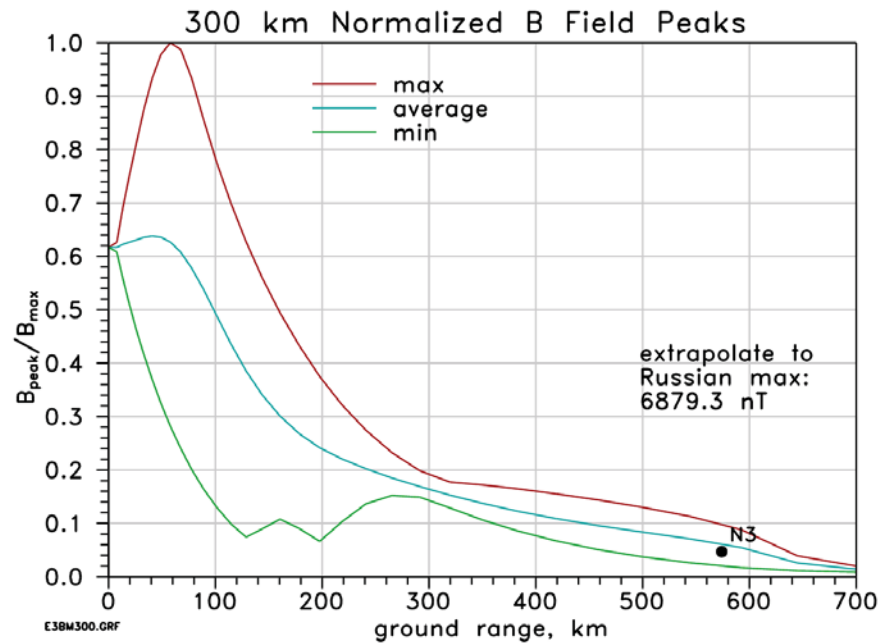


Figure 23 Normalized simulated B field peaks versus ground range for the 300 km test. The black dot shows the simulated results for the N3 point.

As noted, the precise observer azimuth positions are unknown, but the normalized value for the assumed position of the N3 observer is shown (the black dot) using a best-estimate location. Note that at this range there is not as much structure to the azimuth variation as there is closer in, such as at the 120 km range, so there is less uncertainty associated with the exact azimuth position for N3. Another way of stating this is to observe that the contour pattern becomes more circular as the observer is further away from surface zero. Using this pattern, the estimate for the maximum is then given by scaling with the factor of 9.03 ( $1/0.111$ ) from the N3 point to the optimum position. The same method was used for the 300 km burst height, in the plot shown in Figure 23.

Table 4 summarizes the scaling for the two cases. The scaled values are listed in the last column. These are found by multiplying the N3 measurements (the 3<sup>rd</sup> column) by the scaling

Table 4 Pattern (observer position) scaling of the Soviet measurements.

Scaling from N3 up to the Maximum Point				
Case	Soviet Measurements		Scaling	
	N1, B (nT)	N3, B (nT)	Scaling Factor	Max, B (nT)
R2, 150 km	1209.0	856.08	9.03	7732.2
R1, 300 km	1484.0	322.57	21.33	6879.3

factors (4<sup>th</sup> column, given by the reciprocal of the N3 values in Figure 22 and Figure 23). For comparison, the maximum measured values are listed in the 2<sup>nd</sup> column (the N1 points). The fact that these are smaller than the scaled maximum values is an indication that none of the observer points were very close to the optimum position.

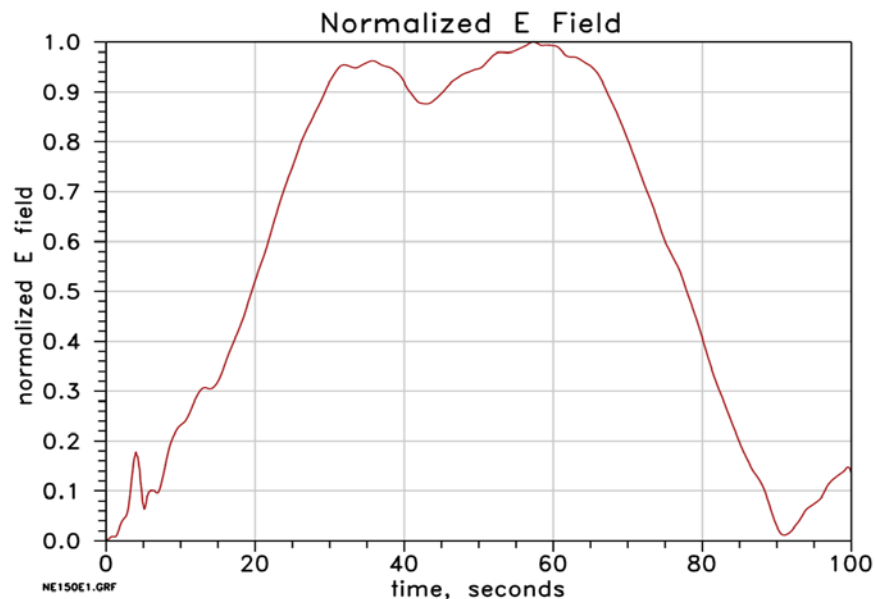
## 4 CONCLUSIONS

The Soviet measurements of the E3 HEMP heave B fields were converted to E fields for a reasonable bounding case of a uniform ground conductivity of 1 mS/m. None of the three measurement points of the E3 HEMP heave fields were near the maximum in the expected field pattern, and column 3 in Table 5 gives estimates of the scaling of the measurements to the expected maximum. The three right columns provide the scaling for magnetic latitude to Hawaii, the southern portion of the continental United States, and Alaska.

*Table 5 Scaling of the Soviet Measurements.*

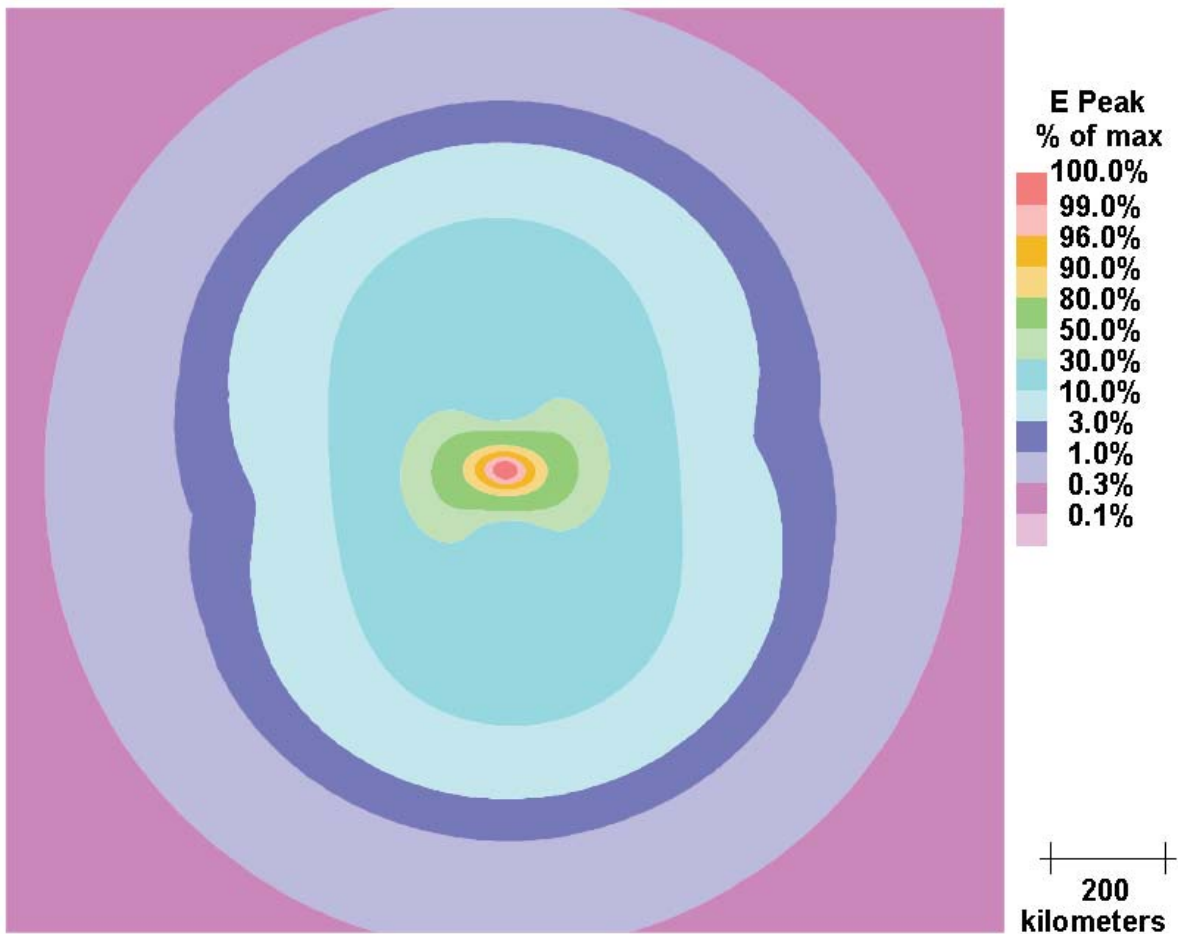
<b>Scaling from N3 up to the Maximum Point, for Three Latitudes for <math>10^{-3}</math> S/m</b>					
Case	Soviet Measurements		Latitude Scaling, E, V/km		
	Latitude (N)	E, V/km	22° N	35° N	65° N
R2, 150 km	48.92°	38.31	64.18	52.24	22.98
R1, 300 km	49.10°	66.39	102.02	84.57	38.28

Figure 24 provides a normalized waveform for one of the E fields. The electric field waveform can be used when computing the induced currents flowing in power lines, for example, to determine the amount of heating in transformer hot spots, as the time dependence of the currents are important in determining thermal effects. Figure 25 provides a sample normalized ground pattern, showing the spatial fall-off from the maximum value. Note that



*Figure 24 E field waveform shape, using the measured N1 waveform from the 150 km burst height*





*Figure 25 Normalized E peak contour pattern from the 150 km burst case*

higher yield bursts could lead to even higher maximum fields, although as shown in the generic curve in Figure 3, the peak value tends to saturate as yields increase. However, this is not true for area coverage, as increasing to larger yields can increase the spatial extent of the high field region.

**From:** [David Andrejcek](#)  
**To:** (b) (6)  
**Subject:** FW: NAS Report on Grid Resilience  
**Date:** Wednesday, January 24, 2018 2:41:52 PM  
**Attachments:** [National Academy of Sciences Enhancing Resilience 2017.pdf](#)

---

Something of interest?

---

**From:** Arnie Quinn  
**Sent:** Wednesday, January 24, 2018 9:33 AM  
**To:** Jette Gebhart <Jette.Gebhart@ferc.gov>; Jignasa Gadani <Jignasa.Gadani@ferc.gov>; Anna Cochrane <Anna.Cochrane@ferc.gov>; Michael Bardee <Michael.Bardee@ferc.gov>; David Ortiz <David.Ortiz@ferc.gov>; James Danly <James.Danly@ferc.gov>; David Morenoff <David.Morenoff@ferc.gov>; Joseph McClelland <Joseph.McClelland@ferc.gov>; David Andrejcek <David.Andrejcek@ferc.gov>  
**Cc:** (b) (6)  
**Subject:** NAS Report on Grid Resilience

Martin talked with Alison Clements after the hearing yesterday and she commended to our attention the National Academies of Sciences, Engineering and Medicine's report on grid resilience. Based on his initial review, Martin thought it would be helpful to us and the team. Here is a pdf. I am going to get a hard copy made from the print shop. Let me know if you'd like one as well and we can do one order.

This PDF is available at <http://nap.edu/24836>

SHARE



## Enhancing the Resilience of the Nation's Electricity System

### DETAILS

170 pages | 8.5 x 11 | PAPERBACK

ISBN 978-0-309-46307-2 | DOI 10.17226/24836

### CONTRIBUTORS

Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System; Board on Energy and Environmental Systems; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine

GET THIS BOOK

FIND RELATED TITLES

Visit the National Academies Press at [NAP.edu](http://NAP.edu) and login or register to get:

- Access to free PDF downloads of thousands of scientific reports
- 10% off the price of print titles
- Email or social media notifications of new titles related to your interests
- Special offers and discounts



Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. ([Request Permission](#)) Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences.

Copyright © National Academy of Sciences. All rights reserved.

# Enhancing the **RESILIENCE** of the Nation's Electricity System

Committee on Enhancing the Resilience of the  
Nation's Electric Power Transmission and Distribution System

Board on Energy and Environmental Systems

Division on Engineering and Physical Sciences

A Consensus Study Report of  
*The National Academies of*  
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS

*Washington, DC*

[www.nap.edu](http://www.nap.edu)

**THE NATIONAL ACADEMIES PRESS**

**500 Fifth Street, NW**

**Washington, DC 20001**

This activity was supported by Grant No. EE-0007045 from the U.S. Department of Energy. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any organization or agency that provided support for the project.

International Standard Book Number 13: 978-0-309-46307-2

International Standard Book Number 10: 0-309-46307-6

Library of Congress Control Number: 2017953067

Digital Object Identifier: <https://doi.org/10.17226/24836>

Additional copies of this publication are available for sale from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; <http://www.nap.edu>.

Copyright 2017 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

Suggested citation: National Academies of Sciences, Engineering, and Medicine. 2017. *Enhancing the Resilience of the Nation's Electricity System*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/24836>.

*The National Academies of*  
**SCIENCES • ENGINEERING • MEDICINE**

The **National Academy of Sciences** was established in 1863 by an Act of Congress, signed by President Lincoln, as a private, nongovernmental institution to advise the nation on issues related to science and technology. Members are elected by their peers for outstanding contributions to research. Dr. Marcia McNutt is president.

The **National Academy of Engineering** was established in 1964 under the charter of the National Academy of Sciences to bring the practices of engineering to advising the nation. Members are elected by their peers for extraordinary contributions to engineering. Dr. C. D. Mote, Jr., is president.

The **National Academy of Medicine** (formerly the Institute of Medicine) was established in 1970 under the charter of the National Academy of Sciences to advise the nation on medical and health issues. Members are elected by their peers for distinguished contributions to medicine and health. Dr. Victor J. Dzau is president.

The three Academies work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The National Academies also encourage education and research, recognize outstanding contributions to knowledge, and increase public understanding in matters of science, engineering, and medicine.

Learn more about the National Academies of Sciences, Engineering, and Medicine at [www.nationalacademies.org](http://www.nationalacademies.org).



*The National Academies of*  
SCIENCES • ENGINEERING • MEDICINE

**Consensus Study Reports** published by the National Academies of Sciences, Engineering, and Medicine document the evidence-based consensus on the study's statement of task by an authoring committee of experts. Reports typically include findings, conclusions, and recommendations based on information gathered by the committee and the committee's deliberations. Each report has been subjected to a rigorous and independent peer-review process and it represents the position of the National Academies on the statement of task.

**Proceedings** published by the National Academies of Sciences, Engineering, and Medicine chronicle the presentations and discussions at a workshop, symposium, or other event convened by the National Academies. The statements and opinions contained in proceedings are those of the participants and are not endorsed by other participants, the planning committee, or the National Academies.

For information about other products and activities of the National Academies, please visit [www.nationalacademies.org/about/whatwedo](http://www.nationalacademies.org/about/whatwedo).

## **COMMITTEE ON ENHANCING THE RESILIENCE OF THE NATION'S ELECTRIC POWER TRANSMISSION AND DISTRIBUTION SYSTEM**

M. GRANGER MORGAN, *Chair*, NAS,<sup>1</sup> Carnegie Mellon University, Pittsburgh,  
Pennsylvania  
DIONYSIOS ALIPRANTIS, Purdue University, West Lafayette, Indiana  
ANJAN BOSE, NAE,<sup>2</sup> Washington State University, Pullman  
W. TERRY BOSTON, NAE, PJM Interconnection (retired), Signal Mountain, Tennessee  
ALLISON CLEMENTS, goodgrid, LLC, Salt Lake City, Utah  
JEFFERY DAGLE, Pacific Northwest National Laboratory, Richland, Washington  
PAUL DE MARTINI, Newport Consulting, Sausalito, California  
JEANNE FOX, Columbia University, New York  
ELSA GARMIRE, Dartmouth College (retired), Santa Cruz, California  
RONALD E. KEYS, United States Air Force (retired), Woodbridge, Virginia  
MARK McGRANAGHAN, Electric Power Research Institute, Knoxville, Tennessee  
CRAIG MILLER, National Rural Electric Cooperative Association, Alexandria, Virginia  
THOMAS J. OVERBYE, Texas A&M University, College Station  
WILLIAM H. SANDERS, University of Illinois, Urbana-Champaign  
RICHARD E. SCHULER, Cornell University, Ithaca, New York  
SUSAN TIERNEY, Analysis Group, Aurora, Colorado  
DAVID G. VICTOR, University of California, San Diego

### **Staff**

K. JOHN HOLMES, Study Director  
DANA CAINES, Financial Manager  
ELIZABETH EULLER, Senior Program Assistant (until June 2016)  
JORDAN D. HOYT, Christine Mirzayan Science and Technology Policy Graduate Fellow  
LANITA JONES, Administrative Coordinator (until August 2017)  
JANKI U. PATEL, Program Assistant  
BEN A. WENDER, Program Officer  
E. JONATHAN YANGER, Research Associate (until April 2017)  
JAMES J. ZUCCHETTO, Senior Scientist

---

<sup>1</sup> NAS, National Academy of Sciences.

<sup>2</sup> NAE, National Academy of Engineering.

NOTE: See Appendix C, Disclosure of Conflicts of Interest.

**BOARD ON ENERGY AND ENVIRONMENTAL SYSTEMS**

JARED L. COHON, *Chair*, NAE,<sup>1</sup> Carnegie Mellon University, Pittsburgh, Pennsylvania

DAVID T. ALLEN, NAE, University of Texas, Austin

W. TERRY BOSTON, NAE, PJM Interconnection (retired), Signal Mountain, Tennessee

WILLIAM BRINKMAN, NAS,<sup>2</sup> Princeton University, New Jersey

EMILY A. CARTER, NAS/NAE, Princeton University, New Jersey

BARBARA KATES-GARNICK, Tufts University, Medford, Massachusetts

JOANN MILLIKEN, Independent Consultant, Alexandria, Virginia

MARGO TSIRIGOTIS OGE, Environmental Protection Agency (retired), McLean, Virginia

JACKALYNE PFANNENSTIEL,<sup>3</sup> Independent Consultant, Piedmont, California

MICHAEL P. RAMAGE, NAE, ExxonMobil Research and Engineering Company (retired), New York

DOROTHY ROBYN, Independent Consultant, Washington, D.C.

GARY ROGERS, Roush Industries, Livonia, Michigan

KELLY SIMS-GALLAGHER, Tufts University, Medford, Massachusetts

MARK THIEMENS, NAS, University of California, San Diego

JOHN WALL, NAE, Cummins Engine Company (retired), Belvedere, California

ROBERT WEISENMILLER, California Energy Commission, Sacramento

**Staff**

K. JOHN HOLMES, Acting Director/Scholar

DANA CAINES, Financial Manager

LANITA JONES, Administrative Coordinator (until August 2017)

MARTIN OFFUTT, Senior Program Officer

JANKI U. PATEL, Program Assistant

BEN A. WENDER, Program Officer

JAMES J. ZUCCHETTO, Senior Scientist

---

<sup>1</sup> NAE, National Academy of Engineering.

<sup>2</sup> NAS, National Academy of Sciences.

<sup>3</sup> Deceased on April 26, 2017.

## Preface

Electricity and the underlying infrastructure for its production, transmission, and distribution are essential to the health and prosperity of all Americans. It is important to make investments that increase the reliability of the power system within reasonable cost constraints. However, the system is complex and vulnerable. Despite all best efforts, it is impossible to avoid occasional, potentially large outages caused by natural disasters or pernicious physical or cyber attacks. This report focuses on large-area, long-duration outages—considered herein as blackouts that last several days or longer and extend over multiple service areas or states. When such major electricity outages do occur, economic costs can tally in the billions of dollars and lives can be lost. Hence, there is a critical need to increase the resilience of the U.S. electric power transmission and distribution system—so that major outages are less frequent, their impacts on society are reduced, and recovery is more rapid—and to learn from these experiences so that performance in the future is better.

The many high-profile electric-service interruptions that have occurred over the past two decades, along with recent efforts to enhance the capabilities of the nation's electricity delivery system, prompted several observers to seek an independent review of the vulnerability and resilience of the nation's electricity delivery system. In its 2014 appropriations for the Department of Energy (DOE), Congress called for an independent assessment to “conduct a national-level comprehensive study on the future resilience and reliability of the nation's electric power transmission and distribution system. At a minimum, the report should include technological options for strengthening the capabilities of the nation's power grid; a review of federal, state, industry, and academic research and development programs; and an evaluation of cybersecurity for energy delivery systems.”<sup>1</sup>

The National Academies of Sciences, Engineering, and Medicine established the Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System to conduct the study. On the basis of this mandate, the National Academies asked the committee to address technical, policy, and institutional factors that might affect how modern technology can be implemented to improve the resilience of the electric system; recommend strategies and priorities for how this might be achieved; and identify barriers to its implementation. The full statement of task for the committee is shown in Appendix A. The biographies of the committee members that authored this report are contained in Appendix B.

Committee members included academicians, retirees from industry, current or former employees of state government agencies, and representatives of other organizations. They brought considerable expertise on the operation and regulation of electric power networks, security, and energy economics. The committee met six times in 2016 and 2017 to gather information from public sources (listed in Appendix D) and to discuss the key issues. It also held several conference calls.

The committee operated under the auspices of the National Academies of Sciences, Engineering, and Medicine's Board on Energy and Environmental Systems and is grateful for the able assistance of K. John Holmes, Linda Casola, Elizabeth Euller, Jordan Hoyt, Janki U. Patel, Ben A. Wender, E. Jonathan Yanger, and James Zucchetto of the National Academies' staff.

---

<sup>1</sup> H.R. 113-486, page 103.



## Acknowledgment of Reviewers

This Consensus Study Report was reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise. The purpose of this independent review is to provide candid and critical comments that will assist the National Academies of Sciences, Engineering, and Medicine in making each published report as sound as possible and to ensure that it meets the institutional standards for quality, objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process.

We thank the following individuals for their review of this report:

Mr. William Ball, Southern Company Services, Inc.,  
 Mr. Joe Brannan, North Carolina Electric Membership Corporation,  
 Dr. L. Berkley Davis, Jr. (NAE), GE Power & Water,  
 Mr. Phillip Harris, Tres Amigas LLC,  
 Dr. James L. Kirtley, Jr. (NAE), Massachusetts Institute of Technology,  
 Dr. Butler W. Lampson (NAS/NAE), Microsoft Research,  
 Mr. Ralph LaRossa, Public Service Electric & Gas Company,  
 Mr. Jason McNamara, CNA,  
 Ms. Diane Munns, Environmental Defense Fund,

Mr. David K. Owens, Edison Electric Institute (retired),  
 Dr. William H. Press (NAS), The University of Texas, Austin  
 Dr. B. Don Russell (NAE), Texas A&M University,  
 Dr. Alberto Sangiovanni-Vincentelli (NAE), University of California, Berkeley,  
 Dr. Edmund O. Schweitzer, III (NAE), Schweitzer Engineering Laboratories, Inc.,  
 Mr. Rich Sedano, Regulatory Assistance Project, and  
 Dr. Paul Stockton, Sonecon, LLC.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations of this report nor did they see the final draft before its release. The review of this report was overseen by Julia M. Phillips, NAE, Sandia National Laboratories (retired), and John G. Kassakian, NAE, Massachusetts Institute of Technology (retired). They were responsible for making certain that an independent examination of this report was carried out in accordance with the standards of the National Academies and that all review comments were carefully considered. Responsibility for the final content rests entirely with the authoring committee and the National Academies.





# Contents

SUMMARY	1
1 INTRODUCTION AND MOTIVATION	8
The Nation Depends on a Resilient Electric System, 8	
Resilience and Reliability Are Not the Same Thing, 9	
The Need for More Resilient Transmission and Distribution Systems, 10	
Improving Resilience Presents Fundamental Challenges, 12	
Structure of the Report, 15	
References, 16	
2 TODAY'S GRID AND THE EVOLVING SYSTEM OF THE FUTURE	17
Introduction, 17	
Electric Industry Structure, Asset Ownership, and Operational Roles and Responsibilities, 17	
Physical Structure and Operation of the High-Voltage Transmission Systems, 25	
Physical Structure and Operation of the Distribution System, 27	
Metrics for Reliability and Resilience, 31	
Near-Term Drivers of Change and Associated Challenges and Opportunities for Resilience, 35	
Longer-Term Drivers of Change and Associated Challenges and Opportunities for Resilience, 42	
Sustaining and Improving the Resilience of a Grid That Is Changing Rapidly and in Uncertain Ways, 47	
References, 47	
3 THE MANY CAUSES OF GRID FAILURE	50
Introduction, 50	
Different Causes Require Different Preparation and Have Different Consequences, 50	
Reviewing the Causes of Outages, 50	
The Life Cycle of a Power Outage, 66	
References, 68	
4 STRATEGIES TO PREPARE FOR AND MITIGATE LARGE-AREA, LONG-DURATION BLACKOUTS	70
Introduction, 70	
Planning and Design, 70	
Operations, 86	
References, 92	

5	STRATEGIES FOR REDUCING THE HARMFUL CONSEQUENCES FROM LOSS OF GRID POWER	94
	Introduction, 94	
	Incentives for Preparedness, 95	
	Planning for Grid Failure, 99	
	Design, 104	
	Distribution System Innovations That Could Enhance Resilience, 106	
	References, 108	
6	RESTORING GRID FUNCTION AFTER A MAJOR DISRUPTION	110
	Introduction, 110	
	General Model for Electricity Restoration, 110	
	Disruptions That Involve Across-the-Board Damage to the Grid and Its Supporting Infrastructure, 114	
	Disruptions That Involve Damage to the Cyber Monitoring and Control Systems, 119	
	Disruptions That Involve Only Physical Damage, 125	
	Disruptions That Cause Both Physical and Cyber Damage, 126	
	Opportunities to Improve Restoration, 126	
	References, 129	
	Annex Tables, 130	
7	CONCLUSIONS	134
	Overarching Insights and Recommendations, 134	
	Summary of Detailed Recommendations, 137	
	References, 141	
APPENDIXES		
A	Statement of Task	143
B	Committee Biographies	144
C	Disclosure of Conflicts of Interest	149
D	Presentations and Committee Meetings	150
E	Examples of Large Outages	152
F	Acronyms	155

## Boxes, Figures, and Tables

### BOXES

- S.1 Causes of Most Electricity System Outages, 2
- 1.1 Examples of Outages on Bulk Power Systems and Their Consequences, 13
- 2.1 Examples of Four Different Electric Operational/Reliability/Ownership Structures, 24
- 2.2 Common Distribution System Reliability Metrics, 32
- 2.3 Federal and State Policy Drivers of Change in the Electric System, 36
- 2.4 Example Comments to the Committee on Distributed Energy Resource and Microgrid Deployments Across the United States, 37
- 3.1 Summary of the Metcalf Substation Attack, 53
- 3.2 Summary of the Cyber Attack on the Ukrainian Grid, 54
- 3.3 Electromagnetic Pulse, 62
- 4.1 Financial and Operational Benefits of Distribution Automation to Chattanooga Electric Power Board, 74
- 4.2 Examples of Electric System Vulnerability to Disruptions in Natural Gas Infrastructure, 76
- 4.3 Select Regulatory Actions Supporting Hardening, Modernization, and Other Preventative Investments, 85
- 5.1 Consequences and Civic Response to Damage Caused by the Ice Storm of January 1998, 98
- 5.2 Superstorm Sandy: Preparation, Emergency Response, and Restoration of Services, 102

### FIGURES

- 1.1 The relative frequency of outages in the U.S. bulk power system over the period from 1984 to 2015, 10
- 1.2 (A) A four-stage process of resilience based on a framing by Flynn (2008) and as illustrated by NIAC (2010); (B) In the case of the hierarchically organized power system, these concepts apply at several

different levels of the system with different specific actions and lessons; and (C) Illustration of scales of resilience processes, 11

- 2.1 The bulk energy system encompasses the facilities and control systems for generation and transmission of electricity but does not include local distribution systems, 18
- 2.2 Map of electric distribution utility service territories in the continental United States, 19
- 2.3 The three large electric interconnections that span the United States, large parts of Canada, and a small part of Mexico, 20
- 2.4 The North American transmission system, 21
- 2.5 Map of regional transmission organizations' (RTO) and independent system operators' (ISO) service areas in the United States and Canada, 22
- 2.6 End consumers can choose their electricity provider in restructured states (green), while other states have suspended restructuring activities (yellow) or never initiated them (white), 22
- 2.7 North American Electric Reliability Corporation reliability coordinators are responsible for ensuring reliability across multiple utility service territories, 23
- 2.8 Fraction of customer meters with advanced meters by state in 2015, 30
- 2.9 Schematic of possible electric system configurations and interactions in the future, 38
- 2.10 Different ways in which the nature and scope of the future regulatory environment might evolve, 43
- 2.11 Different ways in which distributed resources might evolve in the future, 43
- 2.12 Under most state laws, there is legal distinction between a utility that serves a multi-story building with its own distributed energy resource and combined heat and power, as shown at the top of this figure, and the situation in which the same loads are distributed across space and are served by a small microgrid, 44
- 2.13 Climate change can affect, and be affected by, the power system, 45

- 2.14 Possible change in the sources and nature of bulk power, 46
- 3.1 Mapping of events that can cause disruption of power systems, 51
- 3.2 Illustration of distinct types of damages that can affect power systems, 52
- 3.3 U.S. Geological Survey assessment of earthquake hazard across the United States, 53
- 3.4 U.S. coastal locations that have experienced major tsunamis over the course of the past 1,000 years, 55
- 3.5 Summary of the state of knowledge of how the frequency and intensity of various weather events may evolve over time, 55
- 3.6 Map of tornado frequency from 1990 to 2009, 56
- 3.7 Tornadoes show a strong (A) temporal and (B) seasonal variation, 57
- 3.8 In 2006, a cluster of tornadoes caused damage across four states in 10 hours from one super cell, 58
- 3.9 (A) Distribution of freezing rain from 1948 to 2000, (B) slight recent trend toward more events, and (C) best estimate of trend by region, 59
- 3.10 (A) Ice accumulation of several inches on distribution lines caused these poles to collapse, and (B) images from the infamous 1998 ice storm across southeastern Canada and the northeastern United States, 60
- 3.11 Example of a Federal Emergency Management Agency flood map for the Susquehanna River near West Pittston, Pennsylvania, 61
- 3.12 (A) The region of hurricane risk is greatest on the Atlantic and Gulf coasts of the United States and (B) recent years have seen a trend of Atlantic hurricanes becoming more intense, 63
- 3.13 Volcanic hazard map for the region around Mount Rainier, 65
- 3.14 Notional time series of a major power outage divided into six stages, 67
- 4.1 The process of considering and mitigating individual component vulnerability based on cost-performance optimization, 71
- 4.2 (A) Following a major storm that disrupted service on many distribution circuits operated by Chattanooga Electric Power Board, automatic reconfiguration prevented outages for many customers (purple) and significantly reduced the number of circuits requiring manual repairs (green); and (B) such automation has greatly reduced the number of customer-hours (area under the curve) of outage experienced, 73
- 4.3 (A) Installations of utility-scale battery storage have increased substantially over the last 5 years, (B) although growth is concentrated in a few areas and dominated by lithium-ion chemistries, 75
- 4.4 2000-bus synthetic network sited in Texas, 79
- 4.5 Disruption of any material or service that the electricity system relies on can result in loss of electric service and make restoration more challenging, 83
- 4.6 Power system operating states, 86
- 4.7 ISO New England control room, 89
- 5.1 Installation of microgrids in 2015 and expected growth to 2020, 97
- 5.2 Installation of “behind the meter” battery storage systems, 97
- 6.1 Illustration of the general processes of restoration that occur on multiple levels by different institutions with responsibility for electricity restoration, 111
- 6.2 Example of data integration to support advanced data analytics for improved restoration efforts, 116
- 6.3 Three ABB single-phase 345 kV compact replacement transformers being moved from St. Louis, Missouri, to a substation in Houston, Texas, under a Department of Homeland Security demonstration project, 117
- 6.4 Restoration of industrial control systems after a cyber breach, 119

## TABLES

- 2.1 Breakdown of Utilities That Own and Operate Generation, Transmission, or Distribution Infrastructure, 19
- 2.2 Example Resilience Metrics Proposed by the Department of Energy-supported Grid Modernization Laboratory Consortium, 33
- 5.1 The Significant Variation in Estimated Financial Losses Suffered by Different Customer Classes Operating under Different Ambient Conditions as a Function of Varying Outage Duration, 96
- 5.2 The Federal Emergency Management Agency's Matrix Concept Illustrates the High Amount of Interagency and Interdepartmental Coordination Required for Assessing and Responding to Threats to the Nation's Vital Infrastructures, 101
- 6.1 Summary of Selected Recommendations Made by the National Research Council in Its 2012 Report *Terrorism and the Electric Power Delivery System*, Together with the Committee's Assessment of Where Things Now Stand, 124
- 6A.1 Variation in Restoration Activities Across the Six Stages of the Life Cycle of an Outage Characterized by Damage to Physical Components, Monitoring and Control Systems, and Supporting Infrastructure, As Indicated in the Upper Right Corner of Figure 3.2, 130
- 6A.2 Restoration Activities Across the Six Stages of the Life Cycle of an Outage from a Cyber Attack, 133

## Summary

Americans' safety, productivity, comfort, and convenience depend on the reliable supply of electric power. The electric power system is a complex "cyber-physical" system composed of a network of millions of components spread out across the continent. These components are owned, operated, and regulated by thousands of different entities. Power system operators work hard to assure safe and reliable service, but large outages occasionally happen. Given the nature of the system, there is simply no way that outages can be completely avoided, no matter how much time and money is devoted to such an effort. The system's reliability and resilience can be improved but never made perfect. Thus, system owners, operators, and regulators must prioritize their investments based on potential benefits. Most interruptions result from physical damage in a local part of the distribution system caused by weather, accidents, or aging equipment that fails. Less frequently, major storms and other natural phenomena, operations errors, and pernicious human actions can cause outages on the bulk power system (i.e., generators and high-voltage power lines) as well as on distribution systems.

### RESILIENCE IS BROADER THAN RELIABILITY

This report of the Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System focuses on identifying, developing, and implementing strategies to increase the power system's *resilience* in the face of events that can cause large-area, long-duration outages: blackouts that extend over multiple service areas or states and last several days or longer. Resilience is not just about lessening the likelihood that these outages will occur. It is also about limiting the scope and impact of outages when they do occur, restoring power rapidly afterwards, and learning from these experiences to better deal with events in the future.

The power system has been undergoing dramatic changes in technology and governance. In some parts of the United States, power is still supplied by regulated, vertically integrated utilities that generate electricity in large power plants, move that power out over high-voltage transmission systems,

and distribute it to end-use customers—all under that single utility's control. In other parts of the country, electric utilities have been restructured to promote competitive markets, particularly in wholesale power sales between generators and electricity distribution companies. In the more market-oriented parts of the country, high-voltage transmission lines that connect wholesale buyers and sellers are regulated or publicly owned, as are most distribution systems that provide the poles, wires, and equipment to serve retail customers. However, the flows over those wires and customers' responses are increasingly determined by market forces. Efforts to improve resilience must accommodate institutional and policy heterogeneity across the country.

There has been significant growth in instrumentation and automation at the level of the high-voltage, or bulk power, system. This allows the system to operate more efficiently and provides system operators with much better situational awareness; this can improve grid reliability and resilience in the face of outages, but this added complexity can also introduce cybersecurity vulnerabilities. Analogous technological advancements on distribution systems (i.e., "smart grids")—including improved sensing, communication, automation technologies, and advanced metering infrastructure—are occurring piecemeal across the country.

In some states, such as Hawaii and California, distributed energy resources, including distributed generation, demand response, energy efficiency, customer-owned storage, microgrids, and electric vehicles, are a rapidly growing fraction of the overall resource mix that must be planned and managed to maintain grid reliability, resilience, and security. However, despite these developments, for at least the next two decades, most U.S. customers will continue to depend on the functioning of the large-scale, interconnected, tightly organized, and hierarchically structured electric grid.

Strategies to enhance electric power resilience must accommodate both a diverse set of technical and institutional arrangements and a wide variety of hazards. There is no "one-size-fits-all" solution to avoiding, planning for, coping with, and recovering from major outages.



## FRAMEWORK AND ORGANIZATION

Chapter 1 provides a brief introduction to the electricity system and motivation for this report. Chapter 2 summarizes the present state of the electricity system and the various ways it may evolve in the future, as well as metrics used to monitor grid reliability and resilience. Chapter 3 identifies, discusses, and compares a range of natural hazards and accidental and pernicious human actions that could cause major disruptions in service. Many of these, listed in Box S.1, have caused outages or impacted electricity system functions at varying scales over the past 30 years, either in the United States or globally. Others hold the potential to become major causes of disruption in the future.

Building a strategy to increase system resilience requires an understanding of a wide range of preparatory, preventative, and remedial actions, as well as how these impact planning, operation, and restoration over the entire life cycle of different kinds of grid failures. Strategies must be crafted with awareness and understanding of the temporal arc of a major outage, as well as how the needs differ from one type of event to another. It is also important to differentiate between actions designed to make the grid more robust and resilient to failure (e.g., wind-resistant steel or concrete poles rather than wood poles) and those that improve the effectiveness of recovery (e.g., preemptively powering down some pieces of the system to minimize damage). Some actions serve both strategies, some serve one but not the other, and some serve one while inhibiting the other. Similarly, the timing of repairs is different depending on the cause. For example, repairs can begin immediately after a tornado has passed, but flooding following a hurricane can delay the start of repair and impede repair efforts. Good planning and preparation are essential to mitigating, coping with, and recovering from major outages. Both human and technical systems must be designed before grid failure so that the responders can assess the extent of failure and damage, dispatch resources effectively, and draw on established component inventories, supply chains, crews, and communication channels.

## Anticipating and Preparing for Disruption

While the possibility of large-area, long-duration blackouts cannot be totally eliminated, there is much that can be done to decrease their likelihood and reduce their magnitude, should they occur. Chapter 4 assesses a variety of techniques that can be employed before an event occurs in order to enhance system resilience. These include improving the health and reliability of the individual grid components (e.g., through asset health monitoring and preventive- and reliability-centered maintenance), improving system architectures to further reduce the criticality of individual components, better simulating high-impact events, and considering the criticality of the grid's underlying cyber infrastructure. Further work can be done in the area of real-time operations to enhance resilience. This includes improving situational awareness in the control room, with a focus on severe events and an inclusion of the cyber infrastructure, adding more wide-area monitoring and control, and developing control systems that better tolerate both accidental faults and malicious attacks. Finally, there is a need to deal with myriad regulatory entities and incentives to fund resilience investments.

## Mitigating the Impacts of Disruption

While large failures of the bulk power system are rare, some will occur, and restoration can take a long time. It is essential that society prepare for periods of prolonged outage, because many vital public infrastructures—such as heating and cooling, water and sewage pumping, traffic control, financial systems, and many aspects of emergency response and public security—depend on the electric power supply. These issues are explored in Chapter 5. The effects of power outages vary with weather, for different types and locations of users, and over different durations. A central theme of this report is the need to improve how different elements of society perform the difficult task of imagining

### BOX S.1

#### Causes of Most Electricity System Outages (shown in alphabetical order and reviewed in Chapter 3)

Cyber attacks	Hurricanes	Space weather and other electromagnetic threats
Drought and water shortage	Ice storms	Tsunamis
Earthquakes	Major operations errors	Volcanic events
Floods and storm surge	Physical attacks	Wildfires
	Regional storms and tornadoes	

## SUMMARY

the diverse consequences of prolonged power outages. Also important is to ensure that equipment that has been purchased or contracted for backup power supply will be available and reliable when needed.

### Recovering from and Learning after Disruption

After the bulk power system has failed, first responders, utilities, and public agencies must work together to restore service. Recovery involves coordinated activity on the physical side—for example, repairing, replacing, and reconfiguring the hardware of the grid—as well as a variety of activities to rebuild the cyber and industrial control systems. These issues are the focus of Chapter 6. Effective restoration must begin well before the disaster through numerous preparatory activities, including drills and stockpiling of key equipment. Utilities and other electric service personnel must think about how they will assess damage, plan restoration, and marshal and deploy the necessary resources. This is complicated by the fact that restoration processes are starkly different depending on the nature of the event. The keys to restoration are to envision a broad range of threats, work through failure scenarios, plan, and rehearse. Regardless of the cause of the outage, restoration always involves agility, collaboration and communications across multiple institutions, and an understanding of the state of the grid and its supporting systems. Technical readiness is the ultimate determinant of the ability to restore, but technical readiness rests firmly on organizational readiness. A process of continual learning and improvement, informed by detailed incident investigations following large outages, is essential for enhancing the resilience of the grid.

### OVERARCHING INSIGHTS AND RECOMMENDATIONS

No single entity is responsible for, or has the authority to implement, a comprehensive approach to assure the resilience of the nation's electricity system. Because most parties are preoccupied dealing with short-term issues, they neither have the time to think systematically about what could happen in the event of a large-area, long-duration blackout, nor adequately consider the consequences of large-area, long-duration blackouts in their operational and other planning or in setting research and development priorities. Hence the United States needs a process to help all parties better envision the consequences of low-probability but high-impact events precipitated by the causes outlined in Chapter 3 and the system-wide effects discussed in Chapter 5. The specific recommendations addressed to particular parties that are provided throughout the report (especially in Chapters 4 through 6) will incrementally advance the cause

of resilience. However, these alone will be insufficient unless the nation is able to adopt a more integrated perspective at the same time. Hence, in addition to the report's *specific* recommendations, the committee provides a series of overarching recommendations.

One of the best ways to make sure that things already in place will work when they are needed is to conduct drills with other critical infrastructure operators through large-scale, multisector exercises. Such exercises can help illuminate areas where improvements in processes and technologies can substantively enhance the resilience of the nation's critical infrastructure.

**Overarching Recommendation 1:** Operators of the electricity system, including regional transmission organizations, investor-owned utilities, cooperatives, and municipally owned utilities, should work individually and collectively, in cooperation with the Electricity Subsector Coordinating Council, regional and state authorities, the Federal Energy Regulatory Commission, and the North American Electric Reliability Corporation, to conduct more regional emergency preparedness exercises that simulate accidental failures, physical and cyber attacks, and other impairments that result in large-scale loss of power and/or other critical infrastructure sectors—especially communication, water, and natural gas. Counterparts from other critical infrastructure sections should be involved, as well as state, local, and regional emergency management offices.

The challenges that remain to achieving grid resilience are so great that they cannot be achieved by research- or operations-related activities alone. While new technologies and strategies can improve the resilience of the power system, many existing technologies that show promise have yet to be fully adopted or implemented. In addition, more coordination between research and implementation activities is needed, building on the specific recommendations made throughout this report. Immediate action is needed both to implement available technological and operational changes and to continue to support the development of new technologies and strategies.

**Overarching Recommendation 2:** Operators of the electricity system, including regional transmission organizations, investor-owned utilities, cooperatives, and municipals, should work individually and collectively to more rapidly implement resilience-enhancing technical capabilities and operational strategies that are available today and to speed the adoption of new capabilities and strategies as they become available.

The Department of Energy (DOE) is the federal entity with a mission to focus on the *longer-term* issues of

developing and promulgating technologies and strategies to increase the resilience and modernization of the electric grid.<sup>1</sup> No other entity in the United States has the mission to support such work, which is critical as the electricity system goes through the transformational changes described in this report. The committee views research, development, and demonstration activities that support reliable and resilient electricity systems to constitute a public good. If funding is not provided by the federal government, the committee is concerned that this gap would not be filled either by states or by the private sector. In part this is because the challenges and solutions to ensuring grid resilience are complex, span state and even national boundaries, and occur on time scales that do not align with business models. At present, two offices within DOE have responsibility for issues directly and indirectly related to grid modernization and resilience.

**Overarching Recommendation 3:** However the Department of Energy chooses to organize its programs going forward, Congress and the Department of Energy leadership should sustain and expand the substantive areas of research, development, and demonstration that are now being undertaken by the Department of Energy's Office of Electricity Delivery and Energy Reliability and Office of Energy Efficiency and Renewable Energy, with respect to grid modernization and systems integration, with the explicit intention of improving the resilience of the U.S. power grid. Field demonstrations of physical and cyber improvements that could subsequently lead to widespread deployment are critically important. The Department of Energy should collaborate with parties in the private sector and in states and localities to jointly plan for and support such demonstrations. Department of Energy efforts should include engagement with key stakeholders in emergency response to build and disseminate best practices across the industry.

The U.S. grid remains vulnerable to natural disasters, physical and cyber attacks, and other accidental failures.

**Overarching Recommendation 4:** Through public and private means, the United States should substantially increase the resources committed to the physical components needed to ensure that critical electric infrastructure is robust and that society is able to cope when the grid fails. Some of this investment should focus on making the existing infrastructure more resilient and easier to repair, including the following:

- The Department of Energy should launch a program to manufacture and deploy flexible and transportable three-phase recovery transformer sets that can be pre-positioned around the country.<sup>2</sup> These recovery transformers should be easy to install and use temporarily until conventional transformer replacements are available. This effort should produce sufficient numbers (on the order of tens compared to the three produced by the Department of Homeland Security's RecX program) to provide some practical protection in the case of an event that results in the loss of a number of high-voltage transformers. This effort should complement, instead of replace, ongoing initiatives related to spare transformers.
- State and federal regulatory commissions and regional transmission organizations should then evaluate whether grids under their supervision need additional pre-positioned replacements for critical assets that can help accelerate orderly restoration of grid service after failure.
- Public and private parties should expand efforts to improve their ability to maintain and restore critical services—such as power for hospitals, first responders, water supply and sewage systems, and communication systems.<sup>3</sup>
- The Department of Energy, the Department of Homeland Security, the Electricity Subsector Coordinating Council, and other federal organizations, such as the U.S. Army Corps of Engineers, should oversee the development of more reliable inventories of backup power needs and capabilities (e.g., the U.S. Army Corps of Engineers' mobile generator fleet), including fuel supplies. They should also "stress test" existing supply contracts for equipment and fuel supply that are widely used in place of actual physical assets in order to be certain these arrangements will function in times of major extended outages. Although the federal government cannot provide backup power equipment to everyone affected by a large-scale outage, these

<sup>2</sup> As noted in Chapters 6 and 7, the Department of Energy's Office of Electricity Delivery and Energy Reliability is supporting the development of a new generation of high-voltage transformers that will use power electronics to adjust their electrical properties and hence can be deployed in a wider range of settings. The committee's recommendation to manufacture recovery transformers is not intended to replace that longer-term effort. However, the Department of Energy's new advanced transformer designs will not be available for some time; in the meantime, the system remains physically vulnerable. While in Chapter 6 the committee notes several government and industry-led transformer sharing and recovery programs, it recognizes that high-voltage transformers represent one of the grid's most vulnerable components deserving of further efforts.

<sup>3</sup> In addition to treatment, sewage systems often need to pump uphill. A loss of power can quickly lead to sewage backups. Notably, a high percentage of the hospital backup generators in New York City failed during Superstorm Sandy.

<sup>1</sup> The Department of Homeland Security, the Federal Energy Regulatory Commission, and other organizations also provide critical support and have primacy in certain areas.

## SUMMARY

resources could make significant contributions at select critical loads.

In addition to providing redundancy of critical assets, transmission and distribution system resilience demands the ability to provide rapid response to events that impair the ability of the power system to perform its function. These events include deliberate attacks on and accidental failures of the infrastructure itself, as well as other causes of grid failure, which are discussed in Chapter 3.

**Overarching Recommendation 5:** The Department of Energy, together with the Department of Homeland Security, academic research teams, the national laboratories, and companies in the private sector, should carry out a program of research, development, and demonstration activities to improve the security and resilience of cyber monitoring and controls systems, including the following:

- Continuous collection of diverse (cyber and physical) sensor data;
- Fusion of sensor data with other intelligence information to diagnose the cause of the impairment (cyber or physical);
- Visualization techniques needed to allow operators and engineers to maintain situational awareness;
- Analytics (including machine learning, data mining, game theory, and other artificial intelligence-based techniques) to generate real-time recommendations for actions that should be taken in response to the diagnosed attacks, failures, or other impairments;
- Restoration of control system and power delivery functionality and cyber and physical operational data in response to the impairment; and
- Creation of post-event tools for detection, analysis, and restoration to complement event prevention tools.

Because no single entity is in charge of planning the evolution of the grid, there is a risk that society may not adequately anticipate and address many elements of grid reliability and resilience and that the risks of this system-wide failure in preparedness will grow as the structure of the power industry becomes more atomized and complex. There are many opportunities for federal leadership in anticipating potential system vulnerabilities at a national level, but national solutions are then refined in light of local and regional circumstances. Doing this requires a multistep process, the first of which is to anticipate the myriad ways in which the system might be disrupted and the many social, economic, and other consequences of such disruptions. The second is to envision the range of technological and organizational innovations that are affecting the industry (e.g., distributed generation and storage) and how such developments may affect the system's reliability and resilience. The

third is to figure out what upgrades should be made and how to cover their costs. For simplicity, the committee will refer to this as a "visioning process." While the Department of Homeland Security (DHS) has overarching responsibility for infrastructure protection, DOE, as the sector-specific agency for energy infrastructure, has a legal mandate and the deep technical expertise to work on such issues.

**Overarching Recommendation 6:** The Department of Energy and the Department of Homeland Security should jointly establish and support a "visioning" process with the objective of systematically imagining and assessing plausible large-area, long-duration grid disruptions that could have major economic, social, and other adverse consequences, focusing on those that could have impacts related to U.S. dependence on vital public infrastructures and services provided by the grid.

Because it is inherently difficult to imagine systematically things that have not happened (Fischhoff et al., 1978; Kahneman, 2011), exercises in envisioning benefit from having multiple groups perform such work independently. For example, such a visioning process might be accomplished through the creation of two small national power system resilience assessment groups (possibly at DOE national laboratories and/or other federally funded research and development centers or research universities). However such visioning is accomplished, engagement from staff representing relevant state and federal agencies is essential in helping to frame and inform the work. These efforts can build on the detailed recommendations in this report to identify technical and organizational strategies that increase electricity system resilience in numerous threat scenarios and to assess the costs and financing mechanisms to implement the proposed strategies. Attention is needed not just to the average economy-wide costs and benefits, but also to the distribution of these across different levels of income and vulnerability. It is important that these teams work to identify common elements in terms of hazards and solutions so as to move past a hazard-by-hazard approach to a more systems-oriented strategy. Producing useful insights from this process will require mechanisms to help these groups identify areas of overlap while also characterizing the areas of disagreement. A consensus view could be much less helpful than a mapping of uncertainties that can help other actors—for example, state regulatory commissions and first responders—understand the areas of deeper unknowns.

Of course national laboratories, other federally funded research and development centers, and research universities do not operate or regulate the power system. At the national level, the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) both have relevant responsibilities and authorities.



**Overarching Recommendation 7A:** The Federal Energy Regulatory Commission and the North American Electric Reliability Corporation should establish small system resilience groups, informed by the work of the Department of Energy/Department of Homeland Security “visioning” process, to assess and, as needed, to mandate strategies designed to increase the resilience of the U.S. bulk electricity system. By focusing on the crosscutting impacts of hazards on interdependent critical infrastructures, one objective of these groups would be to complement and enhance existing efforts across relevant organizations.

As the discussions throughout this report make clear, many different organizations are involved in planning, operating, and regulating the grid at the local and regional levels. By design and of necessity in our constitutional democracy, making decisions about resilience is an inherently political process. Ultimately the choice of how much resilience our society should and will buy must be a collective social judgment. It is unrealistic to expect firms to make investments voluntarily whose benefits may not accrue to shareholders within the relevant commercial lifetime for evaluating projects. Moreover, much of the benefit from avoiding such events, should they occur, will not accrue to the individual firms that invest in these capabilities. Rather, the benefits are diffused more broadly across multiple industries and society as a whole, and many of the decisions must occur on a state-by-state basis.

**Overarching Recommendation 7B:** The National Association of Regulatory Utility Commissioners should work with the National Association of State Energy Officials to create a committee to provide guidance to state regulators on how best to respond to identified local and regional power system-related vulnerabilities. The work of this committee should be informed by the national “visioning” process, as well as by the work of other research organizations. The mission of this committee should be to develop guidance for, and provide technical and institutional support to, state commissions to help them to more systematically address broad issues of power system resilience, including decisions as to what upgrades are desirable and how to pay for them. Guidance developed through this process should be shared with appropriate representatives from the American Public Power Association and the National Rural Electric Cooperative Association.

**Overarching Recommendation 7C:** Each state public utility commission and state energy office, working with the National Association of Regulatory Utility Commissioners, the National Association of State Energy Officials, and state and regional grid operators and emergency preparedness organizations, should establish a standing capability to identify vulnerabilities, identify strategies to reduce local vulnerabilities, develop strategies to cover costs of needed

upgrades, and help the public to become better prepared for extended outages. In addition, they should encourage local and regional governments to conduct assessments of their potential vulnerabilities in the event of large-area, long-duration blackouts and to develop strategies to improve their preparedness.

Throughout this report, the committee has laid out a wide range of actions that different parties might undertake to improve the resilience of the United States power system. If the approaches the committee has outlined can be implemented, they will represent a most valuable contribution. At the same time, the committee is aware that the benefits of such actions—avoiding large-scale harms that are rarely observed—are easily eclipsed by the more tangible daily challenges, pressures on budgets, public attention, and other scarce resources. Too often in the past, the United States has made progress on the issue of resilience by “muddling through” (Lindblom, 1959). Even if the broad systematic approach outlined in this report cannot be fully implemented immediately, it is important that relevant organizations develop analogous strategies so that when a policy window opens in the aftermath of a major disruption, well-conceived solutions are readily available for implementation (Kingdon, 1984).

## SPECIFIC RECOMMENDATIONS

The committee assessed potential threats to the grid, and the conditions on the grid, and provides findings and recommendations throughout the report. In Chapter 7, these specific recommendations are summarized and sorted in terms of the issues they address and the entities to which they are directed. The high-level descriptions of each are listed below. The specific actions that should be taken to implement each one are laid out in Chapter 7.

**Recommendation 1 to DOE:** Improve understanding of customer and societal value associated with increased resilience and review and operationalize metrics for resilience. (Recommendations 2.1 and 2.2)

**Recommendation 2 to DOE:** Support research, development, and demonstration activities to improve the resilience of power system operations and recovery by reducing barriers to adoption of innovative technologies and operational strategies. (Recommendations 4.1, 4.6, 6.5, and 6.7)

**Recommendation 3 to DOE:** Advance the safe and effective development of distributed energy resources and microgrids. (Recommendations 4.2, 5.6, 5.12, and 6.3)

**Recommendation 4 to DOE:** Work to improve the ability to use computers, software, and simulation to research, plan, and operate the power system to increase resilience. (Recommendations 4.3, 4.4, 4.8, 4.9, and 6.12)

## SUMMARY

**Recommendation 5 to DOE:** Work to improve the cyber-security and cyber resilience of the grid. (Recommendations 4.10 and 6.8)

**Recommendation 6 to the electric power sector and DOE:** The owners and operators of electricity infrastructure should work closely with DOE in systematically reviewing previous outages and demonstrating technologies, operational arrangements, and exercises that increase the resilience of the grid. (Recommendations 4.5, 5.10, 6.2, 6.4, and 6.14)

**Recommendation 7 to DHS and DOE:** Work collaboratively to improve preparation for, emergency response to, and recovery from large-area, long-duration blackouts. (Recommendations 3.2, 5.3, 5.5, 6.1, 6.6, and 6.9)

**Recommendation 8 to DHS and DOE:** With growing awareness of the electricity system as a potential target for malicious attacks using both physical and cyber means, DHS and DOE should work closely with operating utilities and other relevant stakeholders to improve physical and cyber security and resilience. (Recommendations 3.1, 6.10, 6.11, and 6.13)

**Recommendation 9 to state offices and regulators:** Work with local utilities and relevant stakeholders to assess readiness of backup power systems and develop strategies to increase investments in resilience enhancing technologies. (Recommendations 5.1, 5.7, 5.9, and 5.11)

**Recommendation 10 to the National Association of Regulatory Utility Commissioners and federal organizations:** Work with DHS and DOE to develop guidance regarding potential social equity implications of resilience investments as well as selective restoration. (Recommendations 5.2, 5.4, and 5.8)

**Recommendation 11 to FERC and the North American Energy Standards Board:** FERC, which has regulatory authority over both natural gas and electricity systems, should address the growing risk of interdependent infrastructure. (Recommendation 4.7)

**Recommendation 12 to NERC:** Review and improve incident investigation processes to better learn from outages that happen and broadly disseminate findings and best practices. (Recommendation 6.15)

## REFERENCES

- Fischhoff, B., P. Slovic, and S. Lichtenstein. 1978. Fault trees: Sensitivity of estimated failure probabilities to problem representation. *Journal of Experimental Psychology: Human Perception and Performance* 4: 342–355.
- Kahneman, D. 2011. *Thinking Fast and Slow*. New York: Farrar, Straus, and Giroux.
- Kingdon, J.W. 1984. *Agendas, Alternatives, and Public Policies*. Boston: Little, Brown, and Company.
- Lindblom, C.E. 1959. The science of muddling through. *Public Administration Review* 19(2): 79–88.



## 1

## Introduction and Motivation

### THE NATION DEPENDS ON A RESILIENT ELECTRIC SYSTEM

The modern world runs on electricity. As individuals, we depend on electricity to heat, cool, and light our homes; refrigerate and prepare our food; pump and purify our water; handle sewage; and support most of our communications and entertainment. As a society, we depend on electricity to light our streets; control the flow of traffic on the roads, rails, and in the air; operate the myriad physical and information supply chains that create, produce, and distribute goods and services; maintain public safety, and help assure our national security.

The incredibly complex system that delivers electricity in the United States was built up gradually. It started with numerous small local systems in the early 1880s and grew to become three large independent synchronous systems<sup>1</sup> that together span the lower 48 United States, much of Canada, and some of Mexico, each of which is one of the largest integrated machines in the world. These interconnected grids have achieved significant gains in efficiency with increasing scale, as well as improved reliability owing to redundant paths over which electricity can flow. Today, power plants using fossil fuels, nuclear energy, and renewable resources supply these machines. They move power to consumers over hundreds of thousands of miles of high-voltage transmission lines and thousands more miles of local distribution lines.

While our society is becoming ever more dependent upon electricity, the electric system is undergoing a complex transformation that includes changing the mix of generation technologies; adding small-scale energy resources connected to the distribution system; incorporating generation and storage on customers' premises; and improving the capability to monitor and control electricity generation, flows, and uses.

While major pollution-control investments and activities have reduced the electric system's environmental impacts over the past century, these impacts remain a problem locally and globally. The need for environmental improvement will continue to be a major force shaping the power system for decades to come. Not only will the electric system continue to shift to a lower-carbon resource mix, but this lower-emission electricity will also be called upon to provide energy to activities, such as transportation and industrial processing, that currently operate on fossil fuels.

Our economy and lifestyles require that electricity be accessible, affordable, reliable, and continuously available. For that to happen, the grid<sup>2</sup> must perform at two levels: (1) The network of high-voltage power lines that spans the country must be able to move power from large generating plants out to local regions; and (2) Lower-voltage distribution systems must be able to move the power to, and occasionally from, factories, businesses, homes, and other end users. The grid must continue to perform these actions as it evolves to accommodate increasing numbers of distributed energy resources, which are often customer-owned, attached to local distribution systems, and have more "smart" technology—the ability to sense and interact with conditions on the grid and with customers' usage patterns and preferences. These many changes are introducing large shifts in the way the system operates. And these changes are occurring during a period of flat or declining growth in electricity generation (EIA, 2016).

For at least the next several decades, few electricity consumers, let alone whole communities, will go completely "off grid." Many consumers will install equipment that meets their needs for at least some of the time. Sometimes they will

<sup>1</sup> As explained in Chapter 2, the U.S. portions of these systems are divided into three interconnections: Eastern, Western, and Texas. Within each interconnection, 60 Hz power is synchronized across the entire system.

<sup>2</sup> Some use "the grid" only to refer to the high-voltage transmission system. Others use "the grid" to refer to the entire system of wires that moves electricity, including the lower-voltage distribution system. In this report, the committee adopts the latter usage. Chapter 2 provides an overview of the physical structure, operation, and governance of both the high-voltage transmission and lower-voltage distribution systems.

## INTRODUCTION AND MOTIVATION

also want to sell surplus power back to the grid. But the fraction of consumers who are able to provide their own resilient electric supply in entirety, without connecting to the grid, will be limited for both economic and social equity reasons.

**Finding:** For at least the next two decades, most customers will continue to depend on the functioning of the large-scale, interconnected, tightly organized, and hierarchically structured electric grid for resilient electric service.

In this context, interruptions in the power supply are disruptive for consumers and for the electric system itself. Interruptions typically arise from physical damage in a local part of the system—for example, lightning strikes, trees that fall on wires, cars or trucks that crash into power poles, or aging equipment that fails. Indeed the majority of the outages that affect the typical customer in the United States in any given year are the result of events that occur to the distribution system. Less frequently, large storms, other natural phenomena, and operator errors cause outages across the large high-voltage, or “bulk power,” system.

A wide variety of events—hurricanes, ice storms, droughts, earthquakes, wildfires, solar storms, and vandalism or malicious attacks on the hardware and software elements of the electric system—can lead to outages. When the power goes out, life becomes difficult. Communications, business operations, and traffic control all become more challenging. If the outage is brief, most people and organizations can and do cope. As the duration and spatial extent of an electricity system outage increase, costs and inconveniences grow. Critical social services—such as medical care, police and other emergency services, and communications systems—can be disrupted and lives can be lost.

This report is about minimizing the adverse impacts of large electric outages through building a resilient electric system.<sup>3</sup> A complex modern economy that depends on reliable electric supply requires a resilient electric system. While any outage can be problematic, in this report the committee focuses on large-area, long-duration outages—blackouts that last several days or longer and extend over multiple service areas or states.

## RESILIENCE AND RELIABILITY ARE NOT THE SAME THING

While utilities work hard to prevent large-scale outages, and to lessen their extent and duration, such outages do occur and cannot be eliminated. Given the many potential

sources of disruption to the power system, what is perhaps surprising is not that large outages occur, but that they are not more common. For decades, the planners and operators of the system have taken care to assure that the electric system is engineered and routinely operated to achieve high levels of reliability. Increasingly, the system’s planners and operators are focusing on resilience as well.

The North American Electric Reliability Corporation (NERC)—the federally approved organization responsible for developing reliability standards for the bulk power system—defines *reliability* in terms of two core concepts:

1. *Adequacy.* The ability of the electricity system to supply the aggregate electrical demand and energy requirements of the end-use customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.
2. *Operating reliability.* The ability of the bulk power system to withstand sudden disturbances, such as electric short circuits or the unanticipated loss of system elements from credible contingencies, while avoiding uncontrolled cascading blackouts or damage to equipment.<sup>4</sup>

In practice, the system is planned and operated to varying reliability standards. The bulk power system achieves a relatively high degree of reliability across the United States as a whole. For example, adequacy of electricity generation capability is usually measured against a one-day-in-ten-years (1-in-10) loss of load standard, which is typically interpreted to mean that the generation reserves must be high enough that voluntary load shedding due to inadequate supply would occur only once in 10 years (Pfeifenberger et al., 2013). By its very nature, however, the highly complex electrical system—the very epitome of a “cyber-physical system”<sup>5</sup>—is spread out all across the continent. Because it is built up

<sup>4</sup> NERC goes on to state, “Regarding adequacy, system operators can and should take controlled actions or procedures to maintain a continual balance between supply and demand within a balancing area. These actions include: Public appeals; Interruptible demand (i.e., customer demand that, in accordance with contractual arrangements, can be interrupted by direct control of the system operator or by action of the customer at the direct request of the system operator); Voltage reductions (also referred to as “brownouts” because lights dim as voltage is lowered); and Rotating blackouts (i.e., the term used when each set of distribution feeders is interrupted for a limited time, typically 20–30 minutes, and then those feeders are put back in service and another set is interrupted, and so on, rotating the outages among individual feeders). All other system disturbances that result in the unplanned or uncontrolled interruption of customer demand, regardless of cause, fall under the heading of operating reliability. When these interruptions are contained within a localized area, they are considered unplanned interruptions or disturbances. When they spread over a wide area of the grid, they are referred to as cascading blackouts—the uncontrolled successive loss of system elements triggered by an incident at any location” (NERC, 2013).

<sup>5</sup> The National Science Foundation describes “cyber-physical systems” as “engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components” (NSF, 2016).

<sup>3</sup> In parallel with the preparation of this report, which was requested by the Department of Energy (DOE), DOE has also been sponsoring a 3-year Grid Modernization Initiative. That initiative includes a project to develop metrics to measure progress on grid modernization. It is pilot-testing metrics on reliability, resilience, flexibility, sustainability, affordability, and security (DOE, 2015; GMLC, 2016). This report focuses specifically on the issue of resilience.

from millions of complex physical, communications, computational, and networked components and systems, there is simply no way it can be made perfectly reliable.

The concepts of reliability differ from *resilience*, which is the focus of this report. *The Random House Dictionary of the English Language* defines resilient as follows: “the power or ability to return to the original form, position, etc. after being bent, compressed, or stretched . . . [the] ability to recover from illness, depression, adversity, or the like . . . [to] spring back, rebound.” Resilience is not just about being able to lessen the likelihood that outages will occur, but also about managing and coping with outage events as they occur to lessen their impacts, regrouping quickly and efficiently once an event ends, and learning to better deal with other events in the future. Also, a detailed analysis of failure data (Figure 1.1) reveals additional insights that will be explored further in the subsequent chapters of this report.

Flynn (2008) has outlined a four-stage framing of the concept of resilience: (1) preparing to make the system as robust as possible in the face of possible future stresses or attacks; (2) relying on resources to manage and ameliorate the consequences of an event once it has occurred; (3) recovering as quickly as possible once the event is over; and (4) remaining alert to insights and lessons that can be drawn (through all stages of the process) so that if and when another event occurs, a better job can be done in all stages.

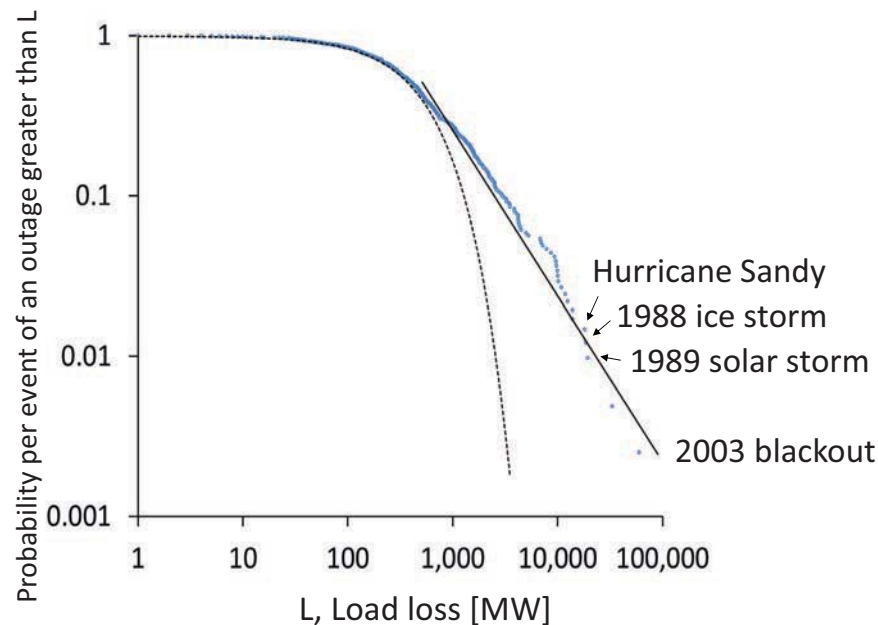
The National Infrastructure Advisory Council created a diagram that illustrates this framing (NIAC, 2010). The committee has adopted this diagram, modifying it only slightly

to add verbs at each stage (Figure 1.2A), and has structured this report to follow these stages. Because the power system is hierarchical, these same concepts apply at several different levels of the system, including at the interconnection, region (some of which are operated by regional transmission organizations), local transmission and distribution systems (typically the domain of utilities), and the end-use level (on the customer side of the meter). Figure 1.2B shows this hierarchy in the abstract, and Figure 1.2C illustrates it for the Western Interconnection. While these figures display a physical hierarchy, there is an analogous hierarchy, but with different boundaries, for the information systems that support sensing and provide control.

**Finding:** Resilience is not the same as reliability. While minimizing the likelihood of large-area, long-duration outages is important, a resilient system is one that acknowledges that such outages can occur, prepares to deal with them, minimizes their impact when they occur, is able to restore service quickly, and draws lessons from the experience to improve performance in the future.

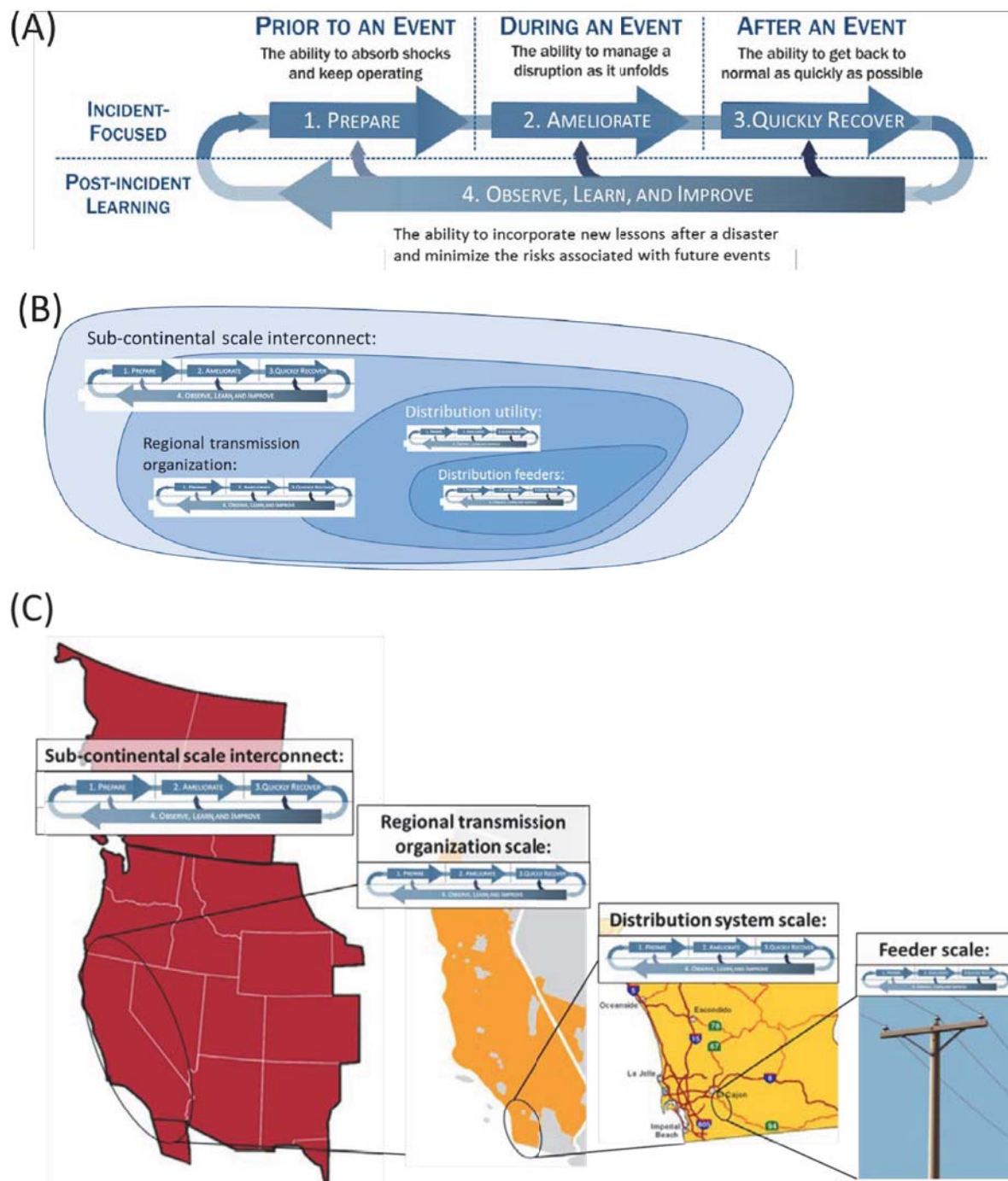
### THE NEED FOR MORE RESILIENT TRANSMISSION AND DISTRIBUTION SYSTEMS

As the committee elaborates in the chapters that follow, the 21st century power system in the United States is not just technically complicated; it is also comprised of diverse and often overlapping institutions and actors. Across the United



**FIGURE 1.1** The relative frequency of outages in the U.S. bulk power system over the period from 1984 to 2015. The figure includes 1,002 events with load loss (loss in electricity demand) greater than 1 MW. The dashed line fits an exponential distribution to the more frequent events with load loss below 500 MW. Note that large outage events do not fit this line and are much more common than one might expect from an extrapolation of the frequency of smaller events. SOURCE: Data are from EIA (2000–2015), NERC (2000–2009), and NRC (2012).

## INTRODUCTION AND MOTIVATION



**FIGURE 1.2** (A) A four-stage process of resilience based on a framing by Flynn (2008) and as illustrated by NIAC (2010); (B) In the case of the hierarchically organized power system, these concepts apply at several different levels of the system with different specific actions and lessons; and (C) Illustration of scales of resilience processes. SOURCE: Modified with permission from NIAC (2010).

States, there are differences in the resilience threats faced by power system operators, in the resources dedicated to mitigating them, and in the capabilities available to utilities and other grid operators in restoring their systems after an outage event. These variations play out in numerous ways. For example, some regions have a single grid operator that

administers competitive wholesale power markets and reliability functions. In other parts of the country, individual utilities dispatch and balance power supplies on their own in response to changing demand. In some states, there are multiple market participants (e.g., generating companies, “wires” companies that transmit power, marketing companies). In



other states, the utilities remain vertically integrated with the same firm having responsibility for both power delivery and generation. Some areas have seen the reliable introduction of many new and different pieces of electrical equipment (e.g., small-scale solar panels, large wind turbines, flywheel storage systems, large-scale electric generating power plants) owned by parties other than the utility or the local grid operator. Other regions are just beginning to manage such changes on the system.

Some utilities have embraced high-speed information and communications technologies to provide them with greater awareness of the state of their system, including the location of outages, while others have made fewer investments in such technologies. Some utilities have substantial resources dedicated to improving cybersecurity while others have close to none. As noted earlier, it is NERC's responsibility to set minimum reliability requirements to address the risks associated with the "weakest link" in the bulk power system. As discussed in more detail in Chapter 2, there is much more variability among states in terms of reliability standards, with individual states setting their own reliability requirements through public utility commissions (and boards for publicly or customer-owned distribution utilities).

Over the past 30 years, numerous headline-making outages have resulted from diverse human and natural causes, including operational errors and meteorological events. A few such outages disrupted electricity service to more than 10,000 MW of customer load (demand).<sup>6</sup> The events that cause outages of this scale leave millions of customers without power, result in economic damages<sup>7</sup> estimated in the billions of dollars, pose serious threats to health and public safety, and could potentially compromise national security. While the United States has fortunately not experienced a major outage caused by a physical or cyber attack, both are a serious and growing risk. Regarding cyber attacks, many attempts to penetrate the system occur every day. Box 1.1 describes four large-area, long-duration outage events that occurred in the past two decades in North America, ranging from the January 1998 ice storm that affected the interconnected power systems in the Northeast United States and

Eastern Canada, to the impacts resulting from Superstorm Sandy in 2012.<sup>8</sup> Box 1.1 also includes description of a cyber attack that disrupted service on the Ukrainian power system in 2015, which did not result in a large-area, long-duration outage but is noteworthy as one of the most prominent examples of cyber disruption of electricity infrastructure. As Box 1.1 makes clear, there is a wide variety of human and natural causes of outages, with significant impacts on economic and human quality of life.

**Finding:** Large-area, long-duration electricity outages that leave millions of customers without power can result in billions of dollars of economic and other damages and cause risk of injury or death. A variety of human and natural events can cause outages with a variety of consequences. The risks of physical or cyber attacks pose a serious and growing threat.

An all-hazards approach to resilience planning is essential, but, with the exception of a few general strategies, there is no "one-size-fits-all" solution to planning for and recovering from major outages. The notion of resilience has to address multiple types of events and operate in a system with multiple overlapping institutions, service providers, grid configurations, ownership structures, and regulatory systems. As outlined above, the system is also comprised of multiple and changing technologies and is constantly evolving. Together this complex physical–cyber–social system is the context and motivation for the National Academies' study presented here.

## IMPROVING RESILIENCE PRESENTS FUNDAMENTAL CHALLENGES

Throughout this report, the committee identifies and discusses a range of technical, institutional, and other strategies that, if adopted, could significantly increase the resilience of the U.S. electric power transmission and distribution systems. It is relatively easy to identify actions and strategies that could improve resilience. Much harder, however, is fostering and realizing the political and organizational support to implement these strategies and actions. The very structure of governance and investment in the electric grid is decentralized. And investment in the grid competes with other social and economic demands as well as for the time and attention of stakeholders. This is especially hard in the face of scarce resources, fragmented government, and the reality that many of the scenarios of large-area, long-duration outages are beyond the realm of experience of most individuals and governing systems.

<sup>6</sup> More than 10,000 MW means more load than that required to power all of New York City. In 2015, the summer coincident peak demand of Zone J (New York City) of the New York grid was 10,410 MW. The population of New York City's five boroughs is 8.5 million people, and the population of the New York City Metropolitan Statistical Area (which includes parts of New Jersey, Connecticut, and Pennsylvania) is more than 20 million. The New York City Metropolitan area accounts for roughly \$1.431 trillion in economic activity (NYISO, 2016; USCB, 2016; IHS Global Insight, 2013).

<sup>7</sup> The events that cause such large-scale outages cause damages to physical structures, including the electricity system, as well as impacts on economic activity. The costs of weather-related power outages are estimated to be billions of dollars annually, with estimates for Superstorm Sandy at \$14–26 billion (EOP, 2013). The potential long-term economic effect of such events in terms of losses and gains in economic activity and accounting for rebound is a more difficult estimate but clearly can be very large.

<sup>8</sup> Most of the damage from Sandy occurred after the winds had dropped below hurricane force and the storm had lost its tropical cyclone characteristics. Thus, the committee uses the term "Superstorm Sandy" and not "Hurricane Sandy" when it refers to this event.

**BOX 1.1****Examples of Outages on Bulk Power Systems and Their Consequences**

The five events summarized below exemplify the types of outages that can result from weather conditions, operational failures, or malicious hacking of the grid. (See Appendix E for a more comprehensive list and description of major outages in the United States.)

**New England/Eastern Canada Ice Storm (1998)**

Between January 4 and January 10, 1998, a series of storms generated along a stationary weather front brought warm Gulf of Mexico precipitation events across a stationary cold air mass (National Weather Service, 1998). While ice storms are common in Eastern Canada, this storm was unique for its long duration (more than 80 hours of freezing rain and drizzle), large geographical extent, and extraordinary freezing rain precipitation totals, with an accumulation of freezing rain greater than 3.1 in (80 mm) thick stretched from southeastern Ontario and northern New York State into southwestern Québec (RMS, 2008). The tremendous weight of accumulated ice resulted in the collapse of 770 electric transmission towers, the replacement of more than 26,000 distribution poles and 4,000 pole-top transformers, and the re-stringing of 1,800 miles of transmission and distribution circuits. At its peak, more than 5.2 million customers in the interconnected areas of Eastern Canada, New York, and New England were without power. Three weeks after the storm, hundreds of thousands of customers still had no power, with some customers not getting power restored until more than 1 month later (RMS, 2008). Storm damage was estimated to be approximately \$4 billion (National Weather Service, 1998).

**Northeast Blackout (2003)**

The August 2003 blackout is the single largest loss of power in U.S. history and was caused by a confluence of factors. A combination of software and operator errors occurring at the Cleveland utility (FirstEnergy) and at the regional reliability coordinator (Midwest Independent Transmission System Operator) greatly reduced the ability of the grid to withstand a reliability event. The regional system operator experienced diminished situational awareness, limiting its ability to intervene to assure system reliability. For example, loss of generation capacity in the Cleveland area adversely affected the ability of key transmission lines into the area to operate at a higher load than usual, but not enough to cause an equipment failure in and of itself. But other factors then triggered outages: contact with overgrown trees in transmission easements into Cleveland ended up tripping several 345 kV lines out of service, and FirstEnergy and Midwest Independent Transmission System Operator were unable to effectively monitor and respond to these losses of electric supply (NERC, 2004). The resulting power flows then redistributed from high-voltage system to lower-voltage lines, leading 16 lines to trip out of service in a 30-minute period, which ultimately caused a cascading collapse of the bulk power system across eight states and two Canadian provinces. The cascading failure left more than 50 million people without power. In certain parts of the outage area, power was not restored for 4 days. The blackout is estimated to have cost between \$4 billion and \$10 billion and contributed to 11 deaths (USCPSOTF, 2004).

**Hurricane Katrina (2005)**

Hurricane Katrina—the all-time most costly weather-related event in the United States—first hit land in Florida as a Category 1 storm, then grew to a Category 5 storm in the Gulf of Mexico before weakening to a strong Category 3 storm at second landfall, with severe storm surges along the Alabama, Mississippi, and Louisiana coastlines (NOAA, 2016). New Orleans experienced devastating flooding and widespread electricity outages, but ultimately damaging storm impacts were felt in eight states across the Southeast (NOAA, 2016). Katrina's impacts included loss of electric service to 2.7 million customers in these states; even 4 weeks after the storm, approximately 250,000 electric customers remained without service (DOE, 2009). In all, the storm destroyed 72,447 utility poles, 8,281 transformers, and 1,515 transmission structures; it took 300 substations off-line, and multiple power plants, including three nuclear plants, either shut down or had to reduce power (DOE, 2009). The flooding in New Orleans prevented full restoration of power for several months. At Southern Company's Mississippi Power, every customer lost power, "nearly two-thirds of the transmission and distribution system was damaged or destroyed, and all but three of the company's 122 transmission lines were out of service. . . . In the distribution system, about 65 percent of facilities were damaged. . . . Mississippi Power's second-largest electricity generating plant was damaged by floodwaters, which affected the company's emergency operations center and backup control center located in the plant. . . . Mississippi Power began tracking Katrina's progress, and 3 days before it hit Mississippi, Mississippi Power began making requests for manpower, material, and logistics. . . . Within 7 days after Katrina, 10,800 workers from 23 states and Canada were assisting Mississippi Power" (Ball, 2006). Katrina's estimated damage ranges from \$84.8 billion to \$157.5 billion (CBO, 2005).

**Superstorm Sandy (2012)**

In October 2012, Superstorm Sandy struck the eastern United States, impacting 24 states in its path. During the 7 days from Sandy's formation to its dissipation, the storm caused swells in excess of 3 meters, flooding in densely populated centers, and extensive damage to infrastructure, with a majority of the damage occurring in New York and New Jersey (FEMA, 2013). Considerable advance notice of the storm allowed electric utilities to make several preemptive steps to mitigate damages, including requests for more assistance from teams from other utility systems, for tree trimming along transmission lines, and for increased readiness of utility outage repair teams (EOP, 2013). It has been estimated that 8 million



customers lost power (Sandalow, 2012). Restoration services reported that 10 to 11 percent of customers in New York and New Jersey remained without power 10 days following the storm. During the outages, 50 deaths were attributed to the lack of electricity, with causes including hypothermia and improperly operated generators. The cost from the post-Sandy power outages has been estimated between \$14 billion and \$26 billion (EOP, 2013).

#### **Cyber Attack on Ukrainian Power Grid (2015)**

In December 2015, a synchronized multi-target cyber attack was executed on three electric grid control centers in eastern Ukraine (DHS, 2016; Volz, 2016). Months previously, the attackers had used “spear-phishing” tactics on employees via a Microsoft Office document to access the corporate networks (E-ISAC and SANS ICS, 2016). The attackers spent the following months learning about the system and its users to gain the necessary credentials to remotely access the communications networks (i.e., supervisory control and data acquisition systems) that control the operation of the electric grid. In December 2015, the attackers began the intrusion by shutting down power to the control center to prevent utility employees from effectively handling the outage (E-ISAC and SANS ICS, 2016). With that response capability compromised, the cyber attackers took control of the electric-system substations themselves and opened substation breakers to shut down power to a larger customer base. Simultaneously, the cyber attackers executed a “denial of service attack” on the customer support facilities, which made the related computer facilities unavailable to customers who sought to report outages and then released malicious software targeted at the master boot record. The attack left approximately 225,000 people without electricity for up to 6 hours. The release of malicious software wiped out personnel computers, servers, and remote terminal units (RTUs), which in turn delayed restoration of service and increased the amount of time required to bring control systems back online. Several substations suffered damage due to the attacks. Although NERC has classified the impacts of these attacks as low due to the short duration of the outage, the relatively small number of infrastructure affected, and the low population percentage of Ukraine that lost power (E-ISAC and SANS ICS, 2016), the attack nonetheless had far-reaching impacts. As of Fall 2016, the utility in Ukraine had yet to reach operational levels experienced prior to the attack, and it is currently unknown when the organization will reach peak operational capabilities again (E-ISAC and SANS ICS, 2016). Thus, in contrast to the other events described here, the Ukraine event was not a long-duration outage event for customers.

Some causes, like major solar coronal mass ejections (see Chapter 3), have very low probabilities of occurrence—sometimes measured in centuries. Others, such as cyber attacks, may become increasingly likely to impact the operations of the grid. Drawing on the tools of decision analysis, an analyst can help a unitary utility-maximizing actor determine how much to spend either to harden a system or to minimize the consequences of disruptive events. However, neither U.S. society, nor its power system, is governed by a single rational actor, but rather is collectively managed by many.

By design and of necessity in our constitutional democracy, making such decisions is an inherently political process. This committee of experts can identify risks and options, outline strategies to improve the understanding of relevant public and private decision makers, and suggest ways to assure that relevant factors are identified and considered. However, ultimately, the choice of how much resilience our society should and will buy must be a collective social judgment.

Large-area, long-duration outages are rare events. And investing in a more resilient system has the classic characteristics of “public goods” issues—localized and concentrated costs with broadly diffused and difficult-to-measure benefits—that are inherently difficult to address. It is unrealistic to expect firms to make voluntary investments whose benefits may not accrue to shareholders within the relevant

commercial lifetime for evaluating projects. Moreover, much of the benefit from avoiding such events, should they occur, will not accrue to the individual firms that invest in these capabilities. Rather, the benefits are diffused more broadly across multiple industries and society as a whole.

In some parts of the United States, rural electric cooperatives, vertically integrated utilities, and utility regulators may be better able to take a longer-term perspective that considers such broader societal benefits. But too often decision makers are pressed by short-term considerations of cost and choices about where expenditures should be directed for various and sometimes competing purposes, and so they must have a strong basis for approving expenses for activities that may not yield benefits for decades or longer. At the national level, the Federal Energy Regulatory Commission and NERC have the ability to adopt a somewhat longer-term perspective, although they too face short-term pressures and fiscal constraints.

No single entity is responsible for assuring the system is resilient in the face of all of them. Strategies to assure more systematic planning and to cover the costs of needed investments are discussed in Chapter 7. Many of the actions designed to reduce system vulnerability to one specific event can actually provide effective protection against a variety of events. For example, in regions where flooding is not an issue, undergrounding power lines can make the system less vulnerable to the impacts of severe storms as well as vehicle

## INTRODUCTION AND MOTIVATION

accidents. This may make such actions and investments easier to justify. Experience demonstrates the normal cycle of public reactions to major events with big impacts on society: there is a tendency not only to identify parties that can be blamed for failing to prevent the event and its impacts, but also to call for greater protective action against exactly the type of event just experienced. Regulators and other decision makers need to have well developed plans that can be implemented during such a “policy window” and designed for robustness against a wide range of threats.

There are some communities at considerably greater risk than others, including those at vulnerable locations in the electricity system or those within or close to natural hazards. When those communities take action, the results can serve as a stimulus and template for others to follow. Some modest government pilot funds to initiate such examples can be a socially prudent investment. At the same time, it is important that the United States devise ways to increase the likelihood that lessons learned from demonstrations can be diffused more widely. National organizations such as the National Association of Regulatory Utility Commissioners, the Edison Electric Institute, the National Rural Electric Cooperative Association, the American Public Power Association, and the National Governors Council can play important roles, raising awareness, sharing best practices, and providing guidance to members. Public and private partnerships such as the Electricity Subsector Coordinating Council, which gained importance following Superstorm Sandy, also serves as a viable forum for enhancing coordination and communication; conducting drills and exercises; and sharing tools and technologies to enhance grid resilience.

Throughout this report, the committee has tried to be attentive to the tension between two competing realities. One is that the electric power system and its regulation are decentralized across the many states and regions. The other is that a coherent strategy will not emerge without stewardship at the federal level and/or from organized leadership from public and private institutional partners that support actions in the national interest. The Department of Homeland Security (DHS) is specifically charged with identifying potential vulnerabilities and assisting in the development and implementation of strategies to reduce risks and increase resilience. However, neither DHS nor the set of local actors that typically interact with DHS control or run the power system. Moreover, the department is stretched very thin and has relatively modest technical expertise in the context of electric power systems.

As the energy sector lead agency and with its focus on research, DOE does have a longer-term perspective and hence is in a position to lay the groundwork and demonstrate the feasibility of a variety of technologies and strategies that, when adopted by others, can considerably enhance the resilience of the grid. Multiple DOE offices have programs related to electric power grid resilience. Specifically, the Office of Electricity Delivery and Energy Reliability and

Office of Energy Efficiency and Renewable Energy have responsibility for directing work on many of the nation's grid modernization and system integration programs and thus have a vital role to play in this area.

The Electric Power Research Institute can also make important contributions—including improving awareness of technologies and practices that are emerging globally—but the amount of fundamental longer-term work they can support is limited. The National Rural Electric Cooperative Association is undertaking a range of research activities that adopt a longer-term perspective. Many states around the country are also working on specific resilience projects, often in the aftermath of those states having experienced disruptive events that have focused policy makers' attention on the issue.

In the chapters that follow, the committee identifies and discusses many things that both the federal government and industry can do to advance the resilience of the power system. In Chapter 7, the committee returns to the broader issues of who is in charge, how electricity system operators, regulators, and society more broadly should choose what is worth doing, and how to pay for it.

## STRUCTURE OF THE REPORT

Chapter 2 describes the nation's electric system as it now exists and as it is integrating and adapting to new technologies and changing regulatory and market environments. This chapter provides context for the rest of the report by describing current conditions and factors affecting grid resilience and discussing how these systems might evolve over the coming decades (even if they are changing in unpredictable ways). Chapter 3 describes the many causes of grid failure: the range and types of threats that can, and at least in some cases definitely will, arise to disrupt the operations of the electric grid. Chapters 4 through 6 discuss ways that grid planners and operators, along with the rest of society, can prepare for and reduce the frequency and duration of disruptions (Chapter 4), manage and mitigate the consequences of outages as they occur (Chapter 5), and restore the system to normal operations as rapidly as possible (Chapter 6). These three chapters identify and discuss things already taking place, things that could improve the performance of each aspect of resilience, and things that deserve further attention from researchers and analysts; from owners, operators, and planners of the grid; and from government policy makers. Discussions of topics such as distributed energy resources and microgrids are spread throughout these chapters. Depending on how they are deployed, distributed energy resources and microgrids can be used for many purposes—they can help mitigate and prevent outages (Chapter 4), can help sustain electricity service to critical facilities during an outage (Chapter 5), and can aid in system restoration (Chapter 6). Throughout these chapters, as well as Chapters 2 and 3, the committee makes many specific recommendations

for strategies to increase the resilience of the U.S. electricity transmission and distribution system. While these specific recommendations will advance this purpose, the committee believes that the nation should adopt a more integrated perspective across the numerous, diverse institutions responsible for the resilience of the electricity system. Thus, the final chapter (Chapter 7) brings together a broader set of overarching recommendations intended to bring such an integrated perspective to the issue of electricity system resilience. The report Summary contains both the overarching recommendations and a synopsis of the chapter-specific recommendations.

## REFERENCES

- Ball, B. 2006. Rebuilding electrical infrastructure along the Gulf Coast: A case study. *The Bridge: Linking Engineering and Society*. Washington, D.C.: National Academy of Engineering.
- CBO (Congressional Budget Office). 2005. Macroeconomic and Budgetary Effects of Hurricanes Katrina and Rita. Testimony before the Committee on Budget. U.S. House of Representatives. October 6.
- DHS (Department of Homeland Security). 2016. "DHS Works with Critical Infrastructure Owners and Operators to Raise Awareness of Cyber Threats." <https://www.dhs.gov/blog/2016/03/07/dhs-works-critical-infrastructure-owners-and-operators-raise-awareness-cyber-threats>. Accessed February 27, 2017.
- DOE (Department of Energy). 2009. *Comparing the Impacts of the 2005 and 2008 Hurricanes on U.S. Energy Infrastructure*. <https://www.ee.netl.doe.gov/docs/HurricaneComp0508r2.pdf>.
- DOE. 2015. *Grid Modernization Multi-Year Program Plan*. <https://energy.gov/sites/prod/files/2016/01/f28/2016%20Grid%20Modernization%20Multi-Year%20Program%20Plan.pdf>.
- EIA (Energy Information Administration). 2000–2015. *Electric Power Monthly*, Table B.2. <https://www.eia.gov/electricity/monthly/backissues.html>. Accessed July 13, 2017.
- EIA. 2016. *Electric Power Annual*. <https://www.eia.gov/electricity/annual/>. Accessed July 13, 2017.
- E-ISAC (Electricity Information Sharing and Analysis Center) and SANS ICS (Industrial Control Systems). 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. [https://ics.sans.org/media/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_5.pdf](https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf).
- EOP (Executive Office of the President). 2013. *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*. [https://energy.gov/sites/prod/files/2013/08/f2/2013%20Grid%20Resiliency%20Report\\_FINAL.pdf](https://energy.gov/sites/prod/files/2013/08/f2/2013%20Grid%20Resiliency%20Report_FINAL.pdf).
- FEMA (Federal Emergency Management Agency). 2013. *Hurricane Sandy FEMA After-Action Report*. [https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy\\_fema\\_aar.pdf](https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf).
- Flynn, S.E. 2008. America the resilient: Defying terrorism and mitigating natural disasters. *Foreign Affairs* 87: 2–8.
- GMLC (Grid Modernization Laboratory Consortium). 2016. "Foundational Metrics Analysis." <https://gridmod.labworks.org/projects/foundational-metrics-analysis>. Accessed February 27, 2017.
- IHS Global Insight. 2013. *U.S. Metro Economies*. <http://www.usmayors.org/metroeconomies/2013/201311-report.pdf>.
- National Weather Service. 1998. *Service Assessment: The Ice Storm and Flood of January 1998*. <http://www.weather.gov/media/publications/assessments/iceflood.pdf>.
- NERC (North American Electric Reliability Corporation). 2000–2009. *Event Analysis: System Disturbance Reports*. <http://www.nerc.com/pal/rrm/ea/System%20Disturbance%20Reports%20DL/Forms/AllItems.aspx>. Accessed July 13, 2017.
- NERC. 2004. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* [http://www.nerc.com/docs/docs/blackout/NERC\\_Final\\_Blackout\\_Report\\_07\\_13\\_04.pdf](http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf).
- NERC. 2013. "Reliability Terminology." <http://www.nerc.com/AboutNERC/Documents/Terms%20AUG13.pdf>.
- NIAC (National Infrastructure Advisory Council). 2010. *A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council*. <https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf>.
- NOAA (National Oceanic and Atmospheric Administration). 2016. "U.S. Billion-Dollar Weather and Climate Disasters 1980–2016." <https://www.ncdc.noaa.gov/billions/events.pdf>.
- NRC (National Research Council). 2012. *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press.
- NSF (National Science Foundation). 2016. "Cyber-Physical Systems." [https://www.nsf.gov/funding/pgm\\_summ.jsp?pmis\\_id=503286](https://www.nsf.gov/funding/pgm_summ.jsp?pmis_id=503286). Accessed February 27, 2017.
- NYISO (New York Independent System Operator). 2016. *2016 Load & Capacity Data*. [http://www.nyiso.com/public/webdocs/markets\\_operations/services/planning/Documents\\_and\\_Resources/Planning\\_Data\\_and\\_Reference\\_Docs/Data\\_and\\_Reference\\_Docs/2016\\_Load\\_Capacity\\_Data\\_Report.pdf](http://www.nyiso.com/public/webdocs/markets_operations/services/planning/Documents_and_Resources/Planning_Data_and_Reference_Docs/Data_and_Reference_Docs/2016_Load_Capacity_Data_Report.pdf).
- Peifenberger, J.P., K. Spees, K. Carden, and N. Wintermante. 2013. *Resource Adequacy Requirements: Reliability and Economic Implications*. The Brattle Group, prepared for the Federal Energy Regulatory Commission. <https://www.ferc.gov/legal/staff-reports/2014/02-07-14-consultant-report.pdf>.
- RMS (Risk Management Solutions). 2008. *The 1998 Ice Storm: 10-Year Retrospective*. [http://forms2.rms.com/rs/729-DJX-565/images/wtr\\_1998\\_ice\\_storm\\_10\\_retrospective.pdf](http://forms2.rms.com/rs/729-DJX-565/images/wtr_1998_ice_storm_10_retrospective.pdf).
- Sandalow, D. 2012. "Hurricane Sandy and Our Energy Infrastructure." <https://energy.gov/articles/hurricane-sandy-and-our-energy-infrastructure>. Accessed February 27, 2017.
- USCB (U.S. Census Bureau). 2016. "Annual Estimates of the Resident Population: April 1, 2010 to July 1, 2015." <https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk>. Accessed February 27, 2017.
- USCPSOTF (U.S.-Canada Power System Outage Task Force). 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. <https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>.
- Volz, D. 2016. "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage." *Reuters*, February 25.

## 2

## Today's Grid and the Evolving System of the Future

### INTRODUCTION

This chapter describes the U.S. electric system as it now exists and discusses how it may evolve over the next several decades. First, the committee provides background on the physical, ownership, legal/regulatory structure, and operational characteristics of the nation's electric system, with an emphasis on transmission and distribution infrastructure. The committee focuses on aspects of the national grid that are relevant for understanding electricity system resilience and the strategies employed to enhance it.<sup>1</sup> This overview of transmission and distribution also highlights the sensing, communications, and control systems that currently exist to support a variety of functions on the grid. Then, the committee describes the complex and dynamic forces driving changes in the electricity sector, both in the near term and the long term.<sup>2</sup> Finally, the committee discusses a variety of ways in which the system may change and some of the implications of these changes for the future resilience of the grid. Together, these conditions and trends set the stage for a subsequent discussion of threats to the system (in Chapter 3) and activities associated with each stage of resilience in the electric system (in Chapters 4 through 6).

Strategies to increase the resilience of today's transmission and distribution systems need to accommodate possible future changes in its character, because most of the physical assets and other pieces of the infrastructure have long lifetimes. Planning to enhance resilience should take this into account, along with the often uncertain ways these systems might evolve over the coming decades.

**Finding:** Approaches to assure resilience should consider that components of electricity infrastructure have long lifetimes and that how the grid and its various institutions,

<sup>1</sup> Readers interested in a more detailed description might look at DOE (2017a), NASEM (2016), DOE (2015), MIT (2011), NRC (2012), and Bakke (2016).

<sup>2</sup> Readers interested in a more detailed description might look at MIT (2016).

technological features, legal structures, and economics will change is inherently uncertain.

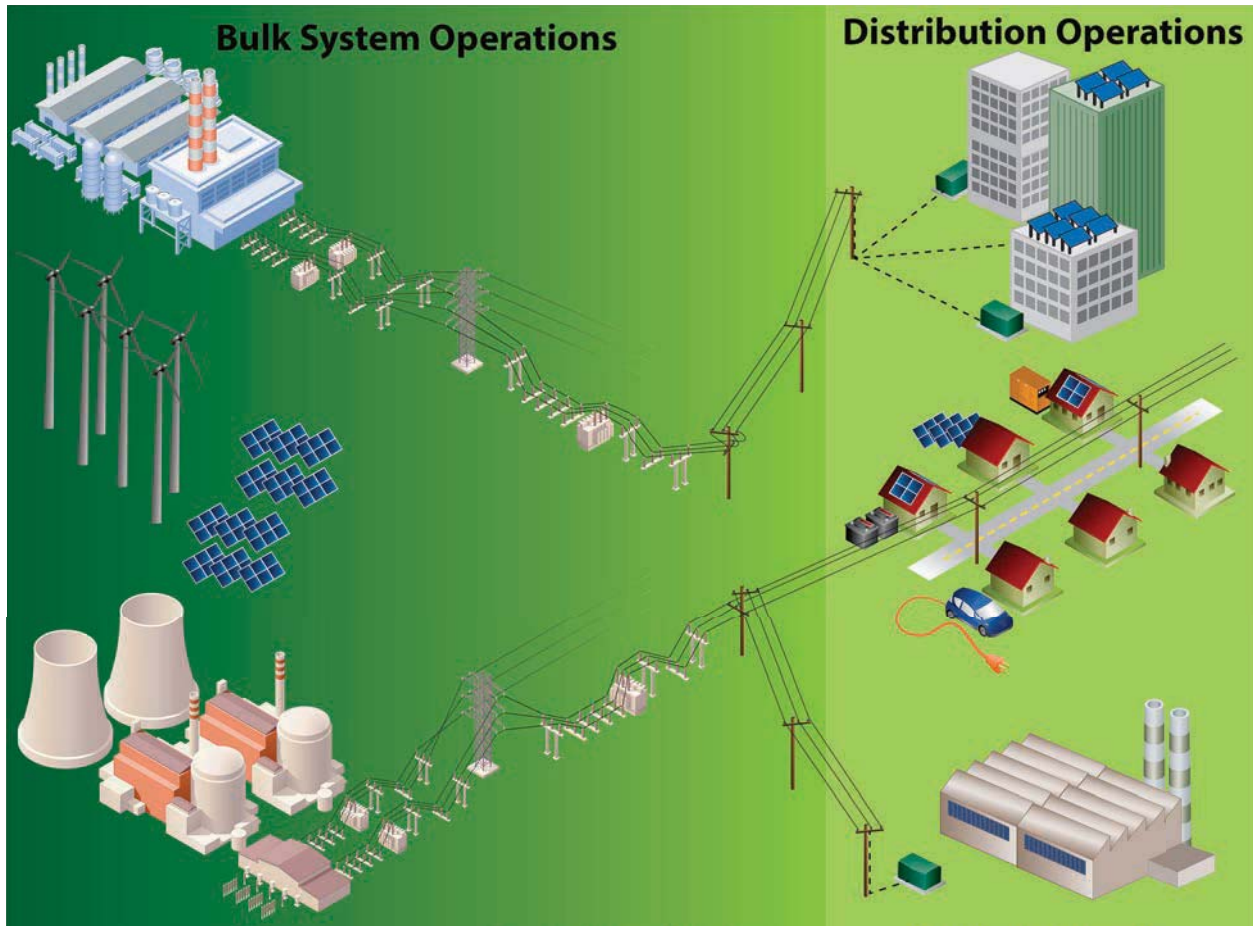
### ELECTRIC INDUSTRY STRUCTURE, ASSET OWNERSHIP, AND OPERATIONAL ROLES AND RESPONSIBILITIES

Since the 1930s in the United States, most electric service to households, businesses, and other customers has been provided by investor-owned or publicly owned electric utilities responsible for all elements of electric supply: generation, transmission at high voltage, and local distribution of power at low voltage. That said, in the first half of the past century the federal government promoted electrification and developed hydropower resources aggressively. This led to the federal government operating several electricity generation and transmission organizations, perhaps the most famous of which are the Tennessee Valley Authority in the southeastern United States and the Bonneville Power Administration in the Pacific Northwest. Figure 2.1 depicts the “bulk energy system,”<sup>3</sup> comprised of central-station power plants and high-voltage transmission lines, and the local “distribution operations” that move power from the bulk system to end-use customers.

Several decades ago, most electric utilities were vertically integrated, meaning that the utility owned the power plants and/or contracts for power; owned or had rights to use high-voltage transmission lines that carry power from remote power plants to their local systems; and owned and operated the low-voltage distribution system to deliver power to consumers. State utility regulators (or, in the case of publicly

<sup>3</sup> The Federal Energy Regulatory Commission has approved the following definition of “bulk energy system” as developed by The North American Electric Reliability Corporation: “All transmission elements operated at 100 kV or higher and real power and reactive power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electrical energy” (NERC, 2016a). There are specific technical exclusions of certain facilities from this definition, but the 100-kV dividing line between bulk energy system (and transmission-level voltage) and lower voltage (and distribution-system-level voltage) is useful for our purposes here.





**FIGURE 2.1** The bulk energy system encompasses the facilities and control systems for generation and transmission of electricity but does not include local distribution systems.

SOURCE: Courtesy of the Electric Power Research Institute. Graphic reproduced by permission from the Electric Power Research Institute from its research report, *The Integrated Grid: A Benefit-Cost Framework*. EPRI, Palo Alto, Calif: 2015. 3002004878.

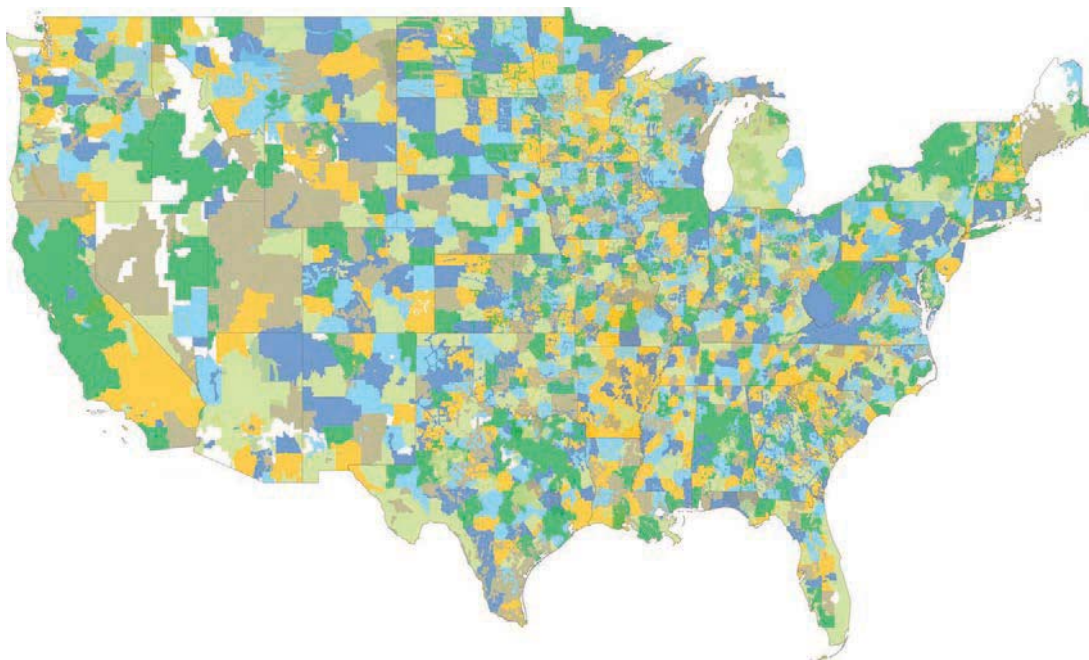
owned utilities, the governing boards of the local utility) set rates for vertically integrated utilities based on the cost of providing service. But nearly 20 years ago, a number of states and federal regulators began to move aggressively to break up vertically integrated utilities, separating the ownership of generation, high-voltage transmission, and distribution systems. In those states, only the distribution part of the system has continued to operate as a regulated monopoly.

As the electric system developed over the decades, investor-owned electric utilities in many parts of the United States merged so as to provide power to customers over larger and larger service territories. In other parts of the country, utilities serve smaller numbers of customers, particularly in rural regions where local electric cooperatives and municipally owned utilities continue to be the dominant providers of electric service. The result is today's patchwork of local distribution utilities (Figure 2.2): thousands of electric utilities provide monopoly service within their local footprint but with a complex system of interconnected facilities that

operates, in effect, as a single "machine" within each interconnection (NAE, 2003).

According to the Energy Information Administration (EIA), there are more than 2,000 utilities that own and/or operate some part of the generation, transmission, or distribution infrastructure in the United States (Table 2.1). More than 70 percent of end-use electricity customers are served by just 174 large investor-owned utilities, while the remaining customers are split roughly evenly between publicly owned utilities and electric cooperatives. Although these investor-owned and publicly owned systems are physically connected, their transmission and distribution systems often have different configurations, voltage ranges, and technology demands; are owned and/or operated by different parties; are subject to different types of regulatory oversight; and are frequently discussed separately.

These many utilities operate as part of three separate interconnected "synchronous" regions within the United States (and parts of Canada), as shown in Figure 2.3. Within



**FIGURE 2.2** Map of electric distribution utility service territories in the continental United States.

SOURCE: Image reproduced with permission from Platts (2014), “Utility Service Areas of North America,” available for purchase online at <https://www.platts.com/products/utility-service-territories-north-america-map>.

each interconnection, the utility systems are physically tied together by major transmission lines. The 60 Hz voltage and current waveforms are synchronized across the entire region, and power flows within each region according to the laws of physics. The three interconnections operate with only a few (asynchronous) direct current (DC) connections that allow transfer of energy between them. The major transmission

lines serving the lower 48 states are shown in Figure 2.4. This figure also illustrates the strong synchronous connection with Canada for both the Eastern and Western interconnections, and the DC lines connecting the asynchronous Québec grid. The integrated North American power system mutually depends on close and continuing collaboration between the United States and Canada. And while there is also a connection to a small portion of Mexico within the Western Interconnection, that dependency is less significant for either country as most of the Mexican grid is a separate system.

Regulation of the electric grid takes place at two levels. The operations, cost allocation, and cost-recovery of the interstate transmission system, as well as wholesale sales of electricity,<sup>4</sup> are largely regulated by the Federal Energy Regulatory Commission (FERC). FERC derives its authorities from the Federal Power Act (FPA), which was initially enacted in 1935 and has been amended multiple times. The second level of regulation occurs on distribution systems that deliver electricity to the end user. The terms and conditions of sales to retail electricity customers, including operations, cost allocation, and cost recovery for local transmission and distribution service, are subject to regulation by state regulatory agencies in those areas served by investor-owned

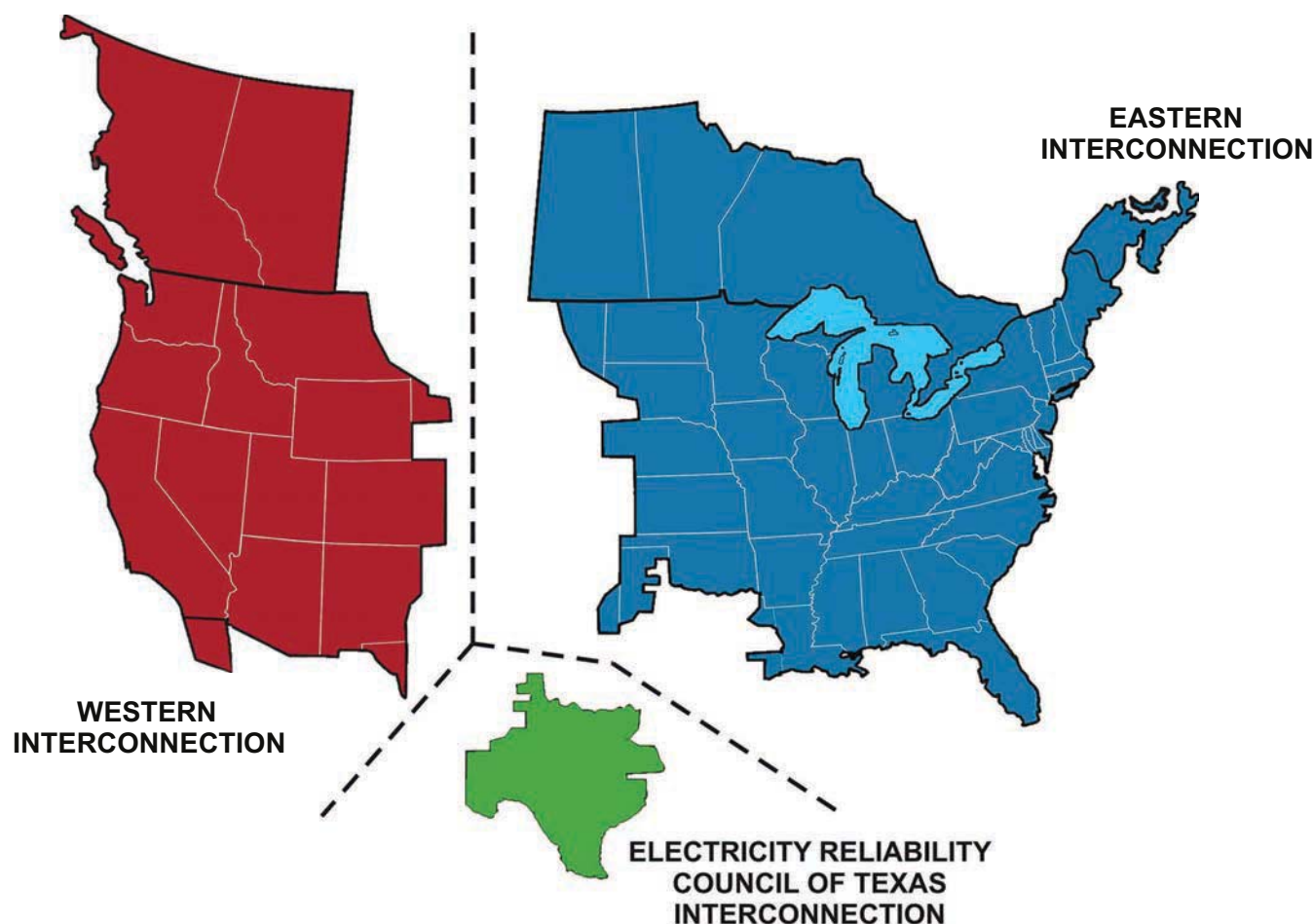
**TABLE 2.1** Breakdown of Utilities That Own and Operate Generation, Transmission, or Distribution Infrastructure

Utility Ownership Structure	Number
Rural electric cooperatives	809
Investor-owned	174
Municipally owned	827
Political subdivision	101
State power authorities	20
Federal utilities/Power marketing administrations	8
Other transmission companies	15
<b>TOTAL</b>	<b>1,954</b>

NOTE: Investor-owned utilities deliver 68 percent of electricity service to retail customers. Cooperatives, municipal utilities, and other publicly owned utilities deliver 13 percent, 12 percent, and 6 percent to retail customers, respectively. (As of 2015, 96 percent of electricity used by customers was sold through utility wires, with 4 percent generated on customers' own premises.) SOURCE: EIA (2016a).

<sup>4</sup> “Wholesale sales of electricity” are sales of power for resale to others, while “retail sales of electricity” are sales to ultimate, end-use customers. Retail sales are typically regulated by state utility regulatory agencies for investor-owned utilities (and by the governing entities of publicly owned or member-owned utilities).





**FIGURE 2.3** The three large electric interconnections that span the United States, large parts of Canada, and a small part of Mexico. A very modest amount of power flows among these three regions over direct current cables so that the 60 Hz power is not synchronized among the regions. Hydro Québec, which is not shown, provides power to many states in the northeastern United States.

SOURCE: DOE (2016a).

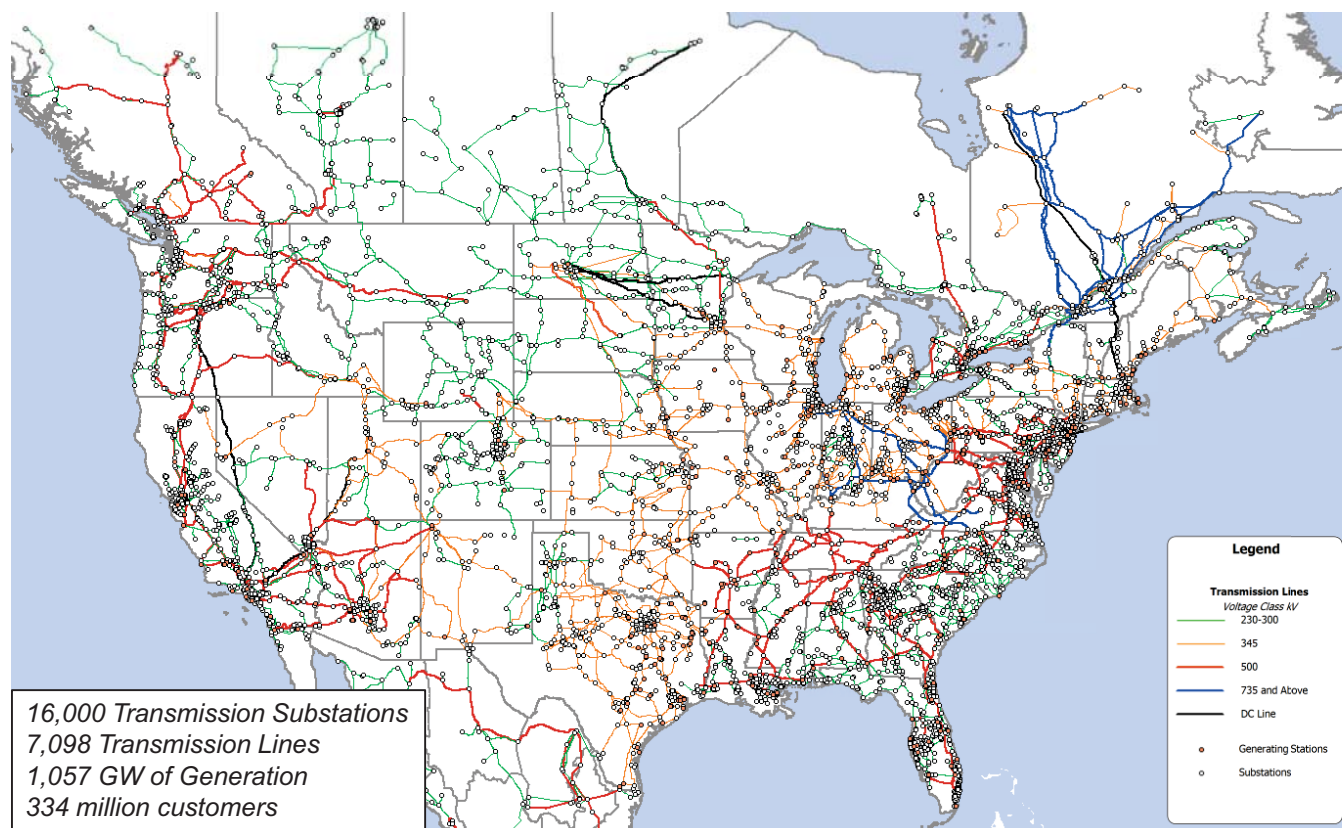
utilities and by publicly accountable boards of public utilities.

This regulatory division between the federal government and the states over the higher- and lower-voltage portions of the electric transmission system first appeared in its current form in the early 20th century and has largely remained in place since then.<sup>5</sup> Although seemingly straightforward, this division of authority is complex in practice and often gives rise to tensions. For example, although the FPA gives FERC authority over transmission service in interstate commerce and wholesale sales of electricity, the states have regulatory authority over siting of transmission lines (including the right to condemn right-of-way). Some states also retain regulatory authority over the costs of transmission as part of the bundled

delivery of retail electricity (in vertically integrated states as described later). Further, many states have the ability to adopt a variety of tax, siting, environmental, and other regulatory policies that affect the mix of power plants in a state.

More than 20 years ago, the electric industry began to undergo pressures for structural change, in part owing to the experiences of deregulating other commercial sectors such as airlines, interstate trucking, and telecommunications. Additional impetus came from federal policies that supported the introduction of relatively small-scale, economical generating technologies owned by non-utility companies, which led to requirements that utilities open up their transmission systems for use by third parties (e.g., the Public Utilities Regulatory Policies Act [PURPA] of 1978). Efforts began in a number of states in the mid-1990s to separate the ownership of generation assets from ownership of the transmission system (the “wires”) and to create competitive wholesale electricity markets. A primary motivation in doing this was a belief that introducing market forces into the industry

<sup>5</sup> As long-distance transmission lines emerged and utilities started to send power onto the grid across long distances, electricity began to cross state lines. Congress created FERC’s predecessor, the Federal Power Commission, in 1935 when it passed the Federal Power Act to address states’ inability to regulate interstate sales of electricity.



**FIGURE 2.4** The North American transmission system.

SOURCE: This information from the North American Electric Reliability Corporation's website is the property of the North American Electric Reliability Corporation and is available at <http://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/2015%20December%20Compiled%20Presentations.pdf>.

would result in lower costs to end users.<sup>6</sup> In fact, creation of competitive wholesale markets in many regions of the country required that non-discriminatory access to transmission infrastructure be provided to all generators. After an initial flurry of “restructuring,” some states began to have second thoughts and decided not to break up their vertically integrated utilities.

Today, there is a patchwork of restructured and vertically integrated utilities across the United States. In much of the country, there are hundreds of non-utility entities involved in the power generation, system operations, power marketing, power trading, and other affiliated activities. The market participants in the electric regions serving two-thirds of the population in the United States are members of organized wholesale electricity markets where a regional transmission organization (RTO) (sometimes called independent system operators [ISOs]) operates the transmission system, prepares regional transmission plans for the market footprint, and conducts competitive product markets (covering energy,

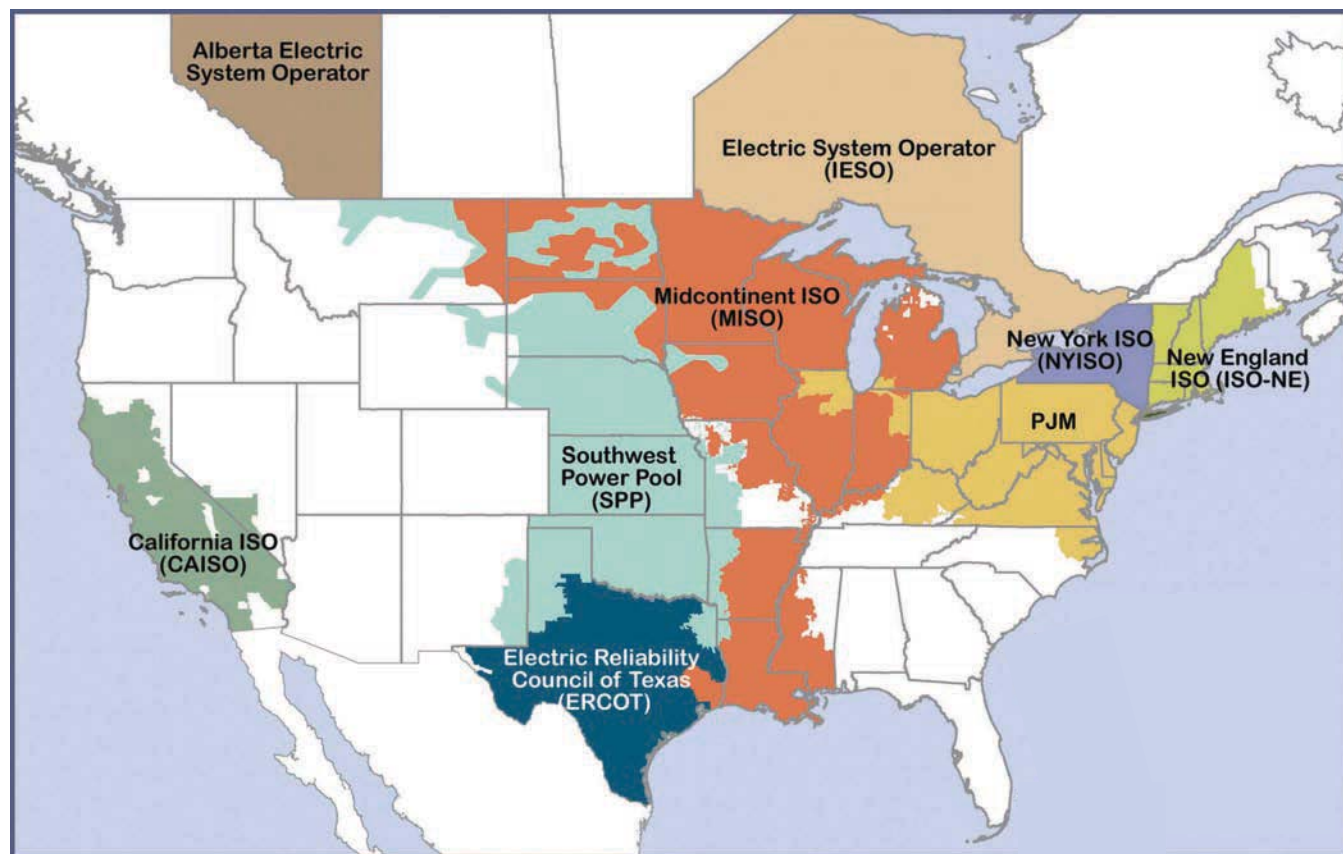
capacity, and/or ancillary services markets).<sup>7</sup> Figure 2.5 shows the boundaries of the current RTOs.

While retaining monopoly ownership of the distribution wires, several states also took steps to open up their electric systems to retail competition. In those shown in green in Figure 2.6, retail customers have the right to choose to buy electricity from competitive retail suppliers. Some states (shown in yellow) took initial steps toward allowing retail choice but then suspended it, while the remaining states (shown in white) did not introduce retail choice.

Across all of these areas, the specific terms and conditions of utility service, and any competitive supply, vary considerably. This makes it very difficult to generalize about industry structure across, and even within, states. At present this heterogeneous “electricity industry” reflects the varied choices that states and localities have made with regard to electric sector structure and regulation. The majority of states retain a vertically integrated structure, pursuant to which retail utilities maintain monopoly status with regard to the

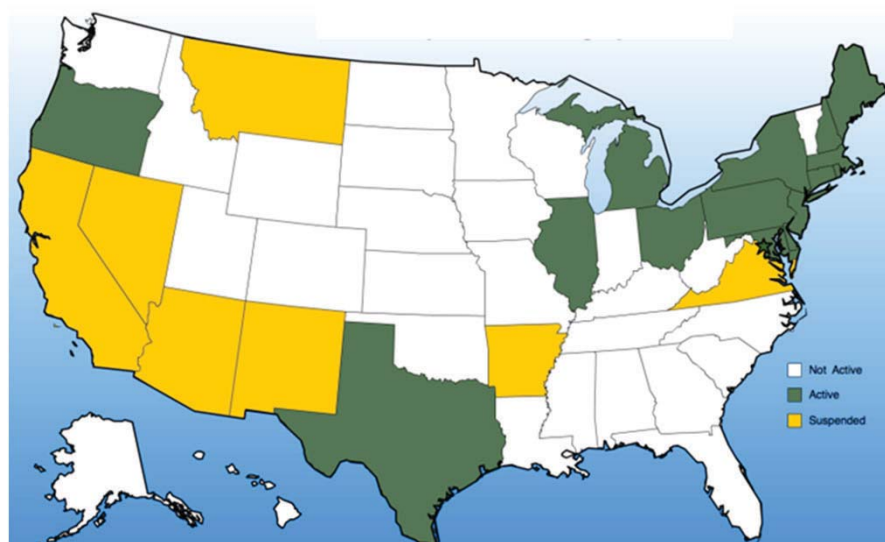
<sup>6</sup> In fact, in most cases, rates did not decrease (Lave et al., 2004; Blumsack et al., 2008).

<sup>7</sup> As of 2015, these seven RTOs served 213.5 million, out of the total estimated U.S. population of 321 million (IRC, 2015; USCB, 2016).



**FIGURE 2.5** Map of regional transmission organizations' (RTO) and independent system operators' (ISO) service areas in the United States and Canada. The parts of the country shown in white do not participate in an RTO, although as of this writing, several utilities in the western states have joined an "Energy Imbalance Market" administered by the California ISO.

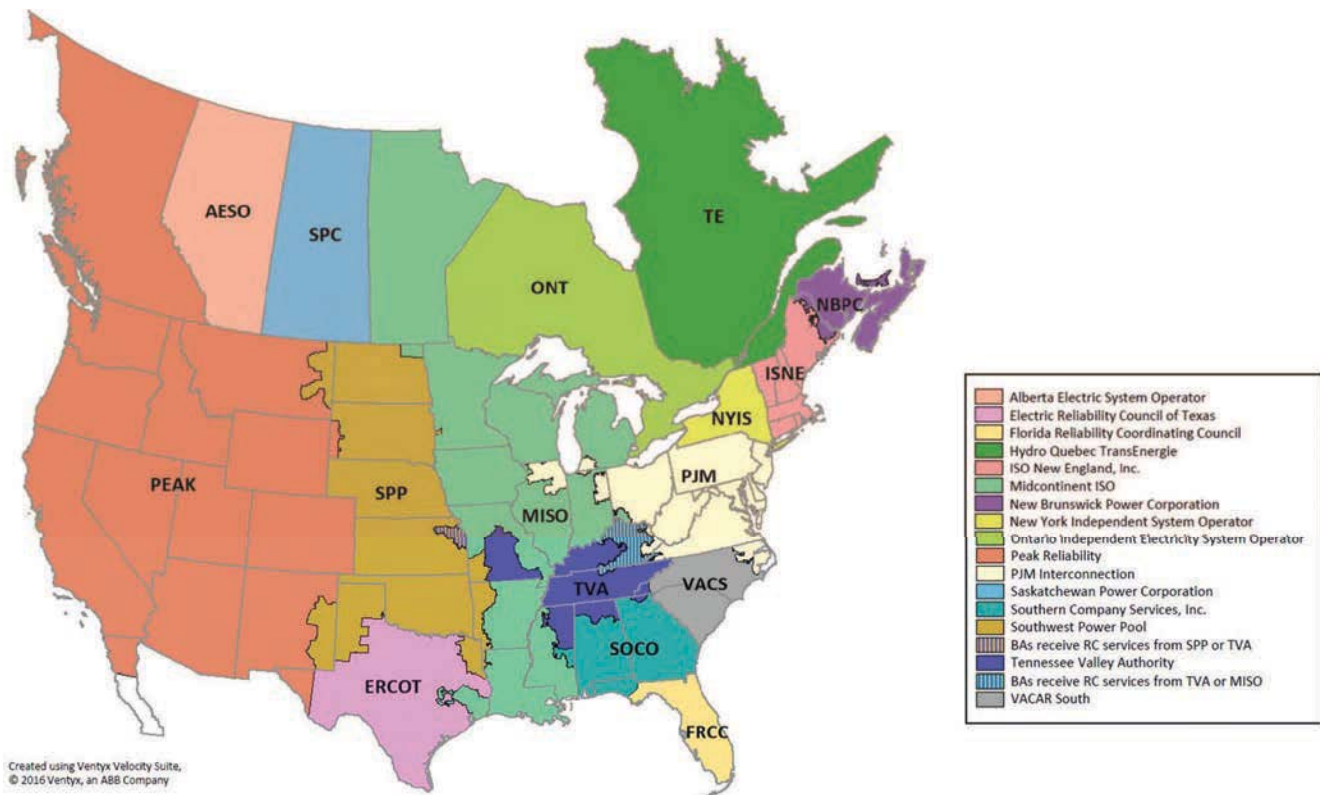
SOURCE: FERC (2016a).



**FIGURE 2.6** End consumers can choose their electricity provider in restructured states (green), while other states have suspended restructuring activities (yellow) or never initiated them (white).

SOURCE: EIA (2010).





**FIGURE 2.7** North American Electric Reliability Corporation reliability coordinators are responsible for ensuring reliability across multiple utility service territories.

SOURCE: This information from the North American Electric Reliability Corporation's website is the property of the North American Electric Reliability Corporation and is available at <http://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx>.

generation, sale, and delivery of electricity. Many states that have vertically integrated utilities without retail choice (e.g., California and many states in the Northern Plains and Upper Midwest) nonetheless have utilities participating in RTOs.

As shown in Figure 2.6, one-third of the states decided to introduce retail choice, and a majority of the states' utilities participate in the competitive generation markets administered by RTOs (shown in Figure 2.5), although the design of these markets varies across the seven RTOs.<sup>8</sup> In some states without retail choice—for example, in Colorado—non-utility companies may own rooftop solar panels that are physically located on a customer's building and sell that power to that customer. But, other such states without retail choice, such as Florida, do not allow anyone besides the utility to sell any form of electricity to consumers, although customers are able to install distributed generation on their premises. As a result of these variations across the states, the regulatory framework under which the electric grid operates takes on several forms. The FPA applies to the entire country but has differing impacts depending on which type of state-regional regulatory regime exists. This complicates

the landscape in which the resilience of the interconnected grid is implemented.

The ownership of transmission infrastructure also varies widely across the United States. In some regions, vertically integrated utilities and large public power providers such as the Bonneville Power Administration and the Tennessee Valley Authority both own and operate the transmission infrastructure. In regions with competitive power markets, operation of the transmission system is delegated to RTOs/ISOs. These organizations may not own the transmission infrastructure under their control, but they are responsible for meeting reliability standards and conducting regional planning efforts, while assuring non-discriminatory access to transmission services for all generators and load-serving entities in the region.

With respect to reliability issues, FERC has responsibility for assuring adherence to mandatory reliability standards for the electric industry. FERC has delegated responsibility for developing reliability standards to the North American Electric Reliability Corporation (NERC), which had originally formed as a voluntary reliability organization following a large blackout in 1965 and is now the designated reliability organization in the United States. NERC develops industry-wide standards, submits them to FERC for approval, and

<sup>8</sup> The only states that do not have any utilities participating in an RTO are Alabama, Alaska, Arizona, Colorado, Florida, Georgia, Hawaii, Idaho, Oregon, South Carolina, Utah, and Washington.

enforces approved standards in the industry. Thus, FERC does not develop reliability standards on its own. Compliance with NERC standards became mandatory with the passage of the 2005 Energy Policy Act (EPAct), and utilities and system operators now face substantial penalties for non-compliance.

Among many other things, NERC has defined the essential system functions necessary to ensure reliability in a framework that accommodates operational and structural differences across regions with and without competitive wholesale markets (NERC, 2010). Within each large region, there is a reliability coordinator with a wide-area perspective on system conditions necessary to ensure that the actions undertaken by one entity do not compromise reliability in another. Currently there are 12 reliability coordinators covering the Continental United States, much of Canada, and a small part of Mexico (Figure 2.7).

Under the purview of these reliability coordinators, more than 100 “balancing authorities” have responsibility for keeping generation and load equal at all times within smaller balancing areas. Regions with a history of tight coordination of operations and planning across utilities within the region, such as New England, New York, and the Mid-Atlantic

region (e.g., Pennsylvania, New Jersey, and Maryland, the original location of the PJM territory), have only a single balancing authority, whereas the majority of reliability coordinators interact with multiple balancing authorities within their footprint. Box 2.1 has examples of transmission system oversight and operation that vary by region.

NERC directs several industry working groups and activities related to preparing for, riding through, and recovering from events with high impacts on the bulk power system. In addition, the Electricity Subsector Coordinating Council (ESCC), formed in response to recommendations from the National Infrastructure Advisory Council, provides a high-level forum for utility executives and federal decision makers to engage and maintain open communication channels in preparation for large-scale outages. To help reduce risks of cyber and physical attacks, for example, NERC operates the Electricity Information Sharing and Analysis Center (E-ISAC), which disseminates information and alerts to electric industry and government representatives, conducts training exercises, and also maintains the Cyber Risk Information Sharing Program that covers nearly 80 percent of operators of the bulk power system. Through the Spare Equipment Working Group, NERC maintains a database of

### BOX 2.1

#### Examples of Four Different Electric Operational/Reliability/Ownership Structures

**Southern Company** (SoCo) is a large vertically integrated utility operating in several Southeastern states. SoCo owns generation assets with a total capacity over 44,000 MW, transmission lines, and four subsidiary distribution utilities. SoCo's electric utilities collectively serve a population of approximately 9 million people (SoCo, 2017). Through these four subsidiaries, SoCo serves the functions of transmission owner, distribution provider, and generation owner while another subsidiary, Southern Company Services, serves as the reliability coordinator, transmission operator, and balancing authority.

**PJM** is an RTO serving all or part of 13 states and the District of Columbia, ranging from Pennsylvania and New Jersey in the East, southward to Virginia, and westward to northern Illinois. PJM provides service in a region with approximately 61 million people and 171,000 MW of generating capacity (PJM, 2017). PJM serves as reliability coordinator, transmission operator, and balancing authority, while also administering the organized competitive wholesale electricity market. However, PJM is not a market participant per se, as other entities own the physical assets associated with generation, transmission, distribution, and power marketing.

**Bonneville Power Administration** (BPA) is a federally operated power marketing administration in the Pacific Northwest, which markets electricity generated from hydroelectric dams owned and operated by the U.S. Army Corps of Engineers or the Bureau of Reclamation (approximately 22,500 MW of capacity), a nuclear power plant, and other renewable generation assets operated by Energy Northwest. BPA's service territory includes Oregon, Washington, western Montana, and small parts of northern California, Nevada, Utah, and Wyoming. BPA owns and operates more than 15,000 circuit miles of transmission (BPA, 2017) and acts as a balancing authority that reports to the regional reliability coordinator. BPA does not own generation or distribution assets.

**Arizona Public Services** (APS) is a vertically integrated utility that owns and operates generation, transmission, and distribution assets. APS provides power to 1.2 million customers in 11 counties in Arizona and generates more than 6,100 MW of capacity (Hoovers, 2017). APS is a balancing authority that reports to the regional reliability coordinator, and, as of the last quarter of 2016, is participating in the Western-states' Energy Imbalance Market administered by the California Independent System Operator (CAISO).

system components, particularly large transformers, which are available to participating utilities should their assets be physically damaged (NERC, 2011). Similar programs are maintained by industry trade organizations, such as the Edison Electric Institute's (EEI) Spare Transformer Exchange Program and the Grid Assurance™ initiative recently launched by the private sector. Parfomak (2014) has prepared an excellent review of the issue of spare transformers for the Congressional Research Service. This report makes it clear that, while the past few years have seen progress, there is still much that needs to be done. The committee returns to the issue of replacement transformers in Chapter 6.

For many years, electric utilities have widely employed mutual-assistance agreements at both the transmission and distribution level to facilitate sharing of skilled workers and equipment to speed restoration efforts following outages. Typically restoration teams are composed with at least one local utility worker so that system-specific and regional knowledge is available on every team. After Superstorm Sandy, EEI developed a National Response Event Framework for pooling resources and coordinating restoration at the nation-scale from outages that overwhelm regional resources (discussed further in Chapter 6).

Thus, a hallmark of the U.S. electric system is that there are a myriad of bodies engaged in the ownership, planning, operation, and regulation of different elements of the system. Although the system itself operates as if it were a unified and coordinated machine, that occurs in spite of—or in the context of—a system in which the many component parts are subject to varied sets of institutional, legal, cultural, and financial incentives and penalties. Asset owners and operators must, and do tend to, operate with awareness of the fact that their systems can be impacted by events and developments occurring on other parts of the machine.

**Finding:** The “electric industry” is different across different parts of the United States in ways that reflect the varied choices that states and localities have made with regard to electric sector structure, asset ownership, and regulation. The specific terms and conditions of utility service, power system planning and operations, and transmission planning vary considerably, making it difficult to generalize about industry structure across and within the states. This complicates the landscape in which the issue of resilience of the interconnected grid must be addressed.

## PHYSICAL STRUCTURE AND OPERATION OF THE HIGH-VOLTAGE TRANSMISSION SYSTEMS

### Physical Structure

Most of the electricity supplied to today's bulk power system is generated by large, central generating stations, often located far from population centers. Roughly one-third of the U.S. electricity supply comes from power plants that

use natural gas, and another one-third comes from coal-fired generation. This reflects a significant increase in gas-fired generation in recent years, up from just 10 percent in 1990 (Tierney, 2016a). The fraction being generated by coal plants has fallen in large part because of competition from low-cost natural gas. Slightly less than 20 percent of generation comes from large nuclear plants. This share has been shrinking slowly, again because of competition from low-cost natural gas (and, to a lesser degree, flat demand and entry of renewable energy technologies) and the high cost of nuclear plant life extension. Hydropower produces 6 percent of the total U.S. power supply, with other renewables accounting for 7 percent of supply—most of that coming from wind (EIA, 2015). While power provided by large-scale wind and solar projects and from equipment such as solar panels located on customers' premises is rapidly growing, it still constitutes a relatively small share of the total supply. These national averages do not reflect that some systems, such as those in California and Hawaii, have much higher percentages of distributed generation and intermittent renewables.

Hundreds of thousands of miles of transmission lines operate in interconnected networks across the United States, which carry alternating current (AC) electricity. Example voltages include 115, 230, 345, 500, and occasionally 765 kV. A few long-distance point-to-point lines use high-voltage direct current (DC) transmission.<sup>9</sup> Electricity moves through the transmission system following the laws of physics and typically cannot be controlled precisely without expensive equipment.<sup>10</sup> The bulk power system relies on large step-up transformers to convert electricity generated at central generating stations to high voltages; this allows for more efficient transmission of power across long distances because there are lower resistive losses of power at higher voltages.

Within the three U.S. bulk-power transmission interconnections, generators operate synchronously at 60 Hz. Large-scale electricity storage is relatively rare;<sup>11</sup> thus, power production and consumption must be kept in balance near instantaneously by increasing or decreasing electricity generation to match changing demand as customers increase and decrease their electricity use. In some areas, in addition to changing the amount of power being generated, grid operators use demand response (DR) programs and technologies to reduce certain loads in lieu of providing more generation. Maintaining the stability of this complex and dynamic

<sup>9</sup> Direct current transmission is used selectively in the United States as a way to transfer power between asynchronous interconnects, occasionally to transfer bulk power over long distances (e.g., from the Pacific Northwest to California and from Labrador to the Northeast United States), and for underwater transmission (e.g., between Connecticut and Long Island and from offshore wind farms).

<sup>10</sup> Technologies that allow control of AC power flows include phase-shifting transformers and other emerging power electronics-based flexible AC transmission system devices that are becoming more available and giving operators more control than ever.

<sup>11</sup> At present, the primary form of large-scale storage capability resides in hydroelectric pumped-storage facilities.



interconnected electric system is an immense operational and technical challenge. Nonetheless, this balancing act is successfully accomplished around-the-clock throughout the grid but not without the complex array of tools, techniques, systems, and equipment dedicated to the task.

The high-voltage transmission network enables power to travel long distances from generating units to substations closer to local end-use customers where the voltage is stepped back down and sent into the distribution system for delivery to consumers. Many of the approximately 15,000 substations have minimal physical protection, exposing them to natural hazards, vandalism, and physical attacks (NERC, 2014). Given that there is no standard design for substations, and especially for the transformers they contain, repairs and replacements of custom-designed facilities can be costly and take many months or even years to complete.

Most power outages occur on the local distribution system. Outages are less frequent on the transmission system. However, when outage events happen on the transmission system, they tend to result in wider impacts and can impose greater costs. Several of the largest outages—introduced in Box 1.1 and listed in greater detail in Appendix E—have resulted from operational or control-system errors followed by equipment tripping off-line due to close proximity with vegetation, as was the case with the 2003 blackout. Given the underlying network configuration of the high-voltage grid, system imbalances caused by events in one place can propagate across the transmission system near instantaneously, with the risk of causing cascading blackouts that impact customers hundreds of miles from the site of the initial disturbance.

**Finding:** Given the interconnected configuration of the high-voltage grid, events in one place can propagate across the transmission system in seconds or a few minutes, potentially causing cascading blackouts that can affect customers hundreds of miles from the initial disturbance. Thus, outage events on the transmission system can result in large-area impacts.

### Sensing, Communication, and Control in the Transmission System

If electricity generation and consumption are not kept in balance, frequency will begin to rise or fall depending on whether there is a surplus or deficit of generated power, respectively. Deviations of voltage or frequency outside of relatively narrow boundaries can lead to physical damage to equipment and can increase the probability of a large-area cascading blackout. System operators depend upon various communications and other systems—for example, supervisory control and data acquisition (SCADA) systems in conjunction with software-based energy management systems (EMS)—to monitor the operating status (or state) of the transmission network and to control specific grid

components to maintain stability. These systems rely on various sensors located primarily at substations (and, to a lesser extent, on transmission lines) to collect and transmit a wide variety of data, including voltage and current characteristics at specific geographic locations; environmental variables such as temperature, wind speed, and ice formation; and measures of asset health such as transformer oil temperature and dissolved gas levels (PNNL, 2015).

Autonomous local controls (called “governors”) at individual generators that boost power output proportional to declining system frequency (and vice versa) are fundamental components of system control responsible for regulating system frequency. The rotational inertia provided by spinning generators and some loads in each interconnection determines the rate of frequency change. On a slower time scale, the 60 Hz frequency is regulated by each balancing authority re-dispatching generation every few seconds through a wide area control scheme called automatic generation control.

Protective relays on the transmission network locate, isolate, and clear faults by triggering the appropriate circuit breakers to disconnect at-risk parts before the system becomes unstable and damage results. Depending upon their vintage, protective relays may be electromechanical (the oldest), solid state, or programmable and microprocessor based. They can act and take effect within tens or hundreds of milliseconds. To maintain acceptable voltage across long distance transmission lines, devices such as capacitor banks and static volt-amp reactive<sup>12</sup> compensators are used to control voltage.

A complex system of communications infrastructure is essential to the reliable operational performance of the electric grid, and this dependence is growing. There is, however, wide variation in the sophistication and speed of communication technologies used across the nation's varied electricity systems, with equipment ranging from twisted wire, to wireless, to rented telephone line, to fiber-optic cable dedicated for utility use. The control of electricity systems is inherently challenging both because changes in the electricity system can occur very rapidly and because control needs to operate over time scales that range from milliseconds to multiple days.

To help system operators maintain system reliability, power systems have sensors, communications, and software that automatically perform analyses so as to constantly monitor the state of the electric system. The overall monitoring and control systems for transmission networks include displays and limit checking of all measurements for operators. A principal tool known as the State Estimator filters the various measurements and estimates the operational characteristics of the power system at regular intervals (e.g.,

<sup>12</sup> Delivered power is the product of voltage and current. In AC systems, only that portion of the current waveform that is in phase with the voltage waveform produces power. However, the out-of-phase current does flow in the lines and causes losses, so utilities strive to keep voltage and current waveforms in phase as close as possible.

every 30 seconds, although the time period used to be longer and continues to get shorter). This helps provide real-time assessments of system conditions that might not otherwise be observable by operators and improves their situational awareness. These assessments also enable other real-time analytic tools that can alert the operator to possible contingencies that could endanger the reliable operation of the grid.

Maintaining the security of these communication networks is critical to the operational integrity of the electricity system. Conversely, the integrity of these other systems (e.g., the internet and communications technologies) depends upon the operational integrity of the electricity system. Conventional approaches to cybersecurity such as firewalls, security software, and “air gaps” (i.e., no connection between systems) are used by utilities to protect their systems from intrusion. However, such measures are being recognized as inadequate, and the growing likelihood that breaches will happen motivates increased emphasis on cyber resilience, including intrusion detection and post-breach restoration. The importance of such activities is illustrated by the 2016 cyber attack on Ukraine’s electricity infrastructure. It took grid operators many months to even recognize that their systems had been compromised, at which point it was too late to prevent substantial outages from occurring.

To date, NERC has mandated nine cybersecurity standards as part of the overall mandatory standards it has established for the electric industry. These critical infrastructure protection (CIP) standards address the security of cyber assets essential to grid reliability.<sup>13</sup> In addition to the cybersecurity standards from the Nuclear Regulatory Commission, these are the only mandatory cybersecurity standards for any of the critical infrastructure sectors across the United States (NERC, 2017).

**Finding:** System operators depend upon SCADA systems in conjunction with software-based EMS to monitor the operating status of the transmission network and to control specific grid components to assure safe and reliable operation. Control is inherently challenging because it must operate over time scales that range from milliseconds to multiple days. Maintaining the security of power system communication

networks and control systems is critical to the operational integrity of the electric system.

**Finding:** CIP standards dictate minimum cybersecurity protections for the bulk power system, and the electricity sector is the only critical infrastructure sector with mandatory standards. However, these standards do not apply to local distribution systems.

## PHYSICAL STRUCTURE AND OPERATION OF THE DISTRIBUTION SYSTEM

### Physical Structure

The electric distribution system moves power from the bulk energy system to the meters of electricity customers. Typically, power is delivered to distribution substations from two or more transmission lines, where it is converted to a lower voltage and sent to customers over distribution feeders. Although distribution system outages tend to be more frequent than those occurring on transmission facilities, the impacts of such outages are smaller in scale and generally easier to repair.

Most local distribution systems in the United States are physically configured as “radial” systems, with their physical layout resembling the trunks and branches of a tree. Customers on radial systems are exposed to interruption when their feeder (i.e., their branch) experiences an outage. In metropolitan areas, these trunks and branches typically have switches that can be reconfigured to support restoration from an outage or regular maintenance. When a component fails in these systems, customers on unaffected sections of the feeder are switched manually or automatically to an adjacent, functioning circuit. However, this still exposes critical services such as hospitals or police stations to potential outages, so these facilities are often connected to a second feeder for redundancy. In high-density urban centers, distribution systems are often configured as “mesh networks,” with a system of interconnected circuits and low-voltage equipment able to provide high reliability service to commercial and high-density residential buildings. Such mesh networks—found in Manhattan, parts of Chicago and San Francisco, and other high-density urban areas—provide multiple pathways through which electric service may be provided to customers.

Most distribution systems’ wires are located above-ground. However, areas with high population density, including some suburban areas, frequently locate electricity and other infrastructure underground. This provides some physical protection and reduces risks posed by vegetation, but it can make identifying faults and implementing repairs more difficult and increase the risk of equipment damage in earthquake and flood-prone locations. In less densely populated areas, distribution feeders are usually located aboveground, with smaller distribution transformers located on local utility

<sup>13</sup> NERC has nine mandatory CIP standards related to cyber issues. These cover such things as reporting of sabotage (CIP-001); identification and documentation of the critical cyber assets associated with critical assets that support reliable operation of the bulk power system (CIP-002); minimum security management controls to protect critical cyber assets (CIP-003); personnel risk assessment, training, and security awareness for personnel with access to critical cyber assets (CIP-004); identification and protection of the electronic security perimeters inside which all critical cyber assets reside, as well as all access points on the perimeter (CIP-005); a physical security program for the protection of critical cyber assets (CIP-006); methods, processes, and procedures for securing critical cyber assets and other cyber assets within the electronic security perimeters (CIP-007); identification, classification, response, and reporting of cybersecurity incidents related to critical cyber assets (CIP-008); and recovery plans for critical cyber assets, relying upon established business continuity and disaster recovery techniques and practices (CIP-009) (NERC, 2017).

poles that step down to lower voltage for delivery to customers' premises.

There is no single organization responsible for establishing or enforcing mandatory reliability standards in distribution systems, although state utility regulators and boards of publicly or customer-owned utilities often assess performance using quantitative reliability metrics and set goals for the allowable frequency and duration of system and customer outages. Typically, utilities collect data on the length and frequency of outages that result from events on the local distribution systems, and some utilities (particularly investor-owned utilities with encouragement from regulators) disclose this information to the public. However, there is wide variation across the states and the utilities within them with regard to their tracking, publication, and/or enforcement of local reliability indicators. In light of their role in approving rates and in deciding what costs and other investments can be recovered through rates, public utility commissions (and boards of publicly or customer-owned distribution utilities) have significant influence on the reliability, cost, and resilience of distribution systems, as FERC does at the bulk energy system level.

In recent years in some parts of the United States, distribution systems have also experienced substantial additions of distributed energy resources (DERs). DERs are electrical resources that are attached to the local distribution system, often behind a customer's meter. Examples include rooftop solar panels, customer-owned batteries, fuel cell technologies, wind turbines, backup generators, and combined heat and power (CHP) systems.<sup>14</sup> Although DERs account for a relatively small fraction of total generation nationally, their installation varies significantly from one state to another, with some local distribution systems (e.g., in Hawaii, California, New Jersey, and Arizona) seeing hundreds of MW of growth in installed capacity in recent years (DOE, 2017a). Because many DERs provide surplus power beyond the amount of electricity consumed on the customer's premises, they inject power into a distribution system designed to operate in a one-way flow of power from the substation to the customer. (See "Near-Term Drivers of Change and Associated Challenges and Opportunities for Resilience" for a longer discussion of DERs and their implications for grid planning, operation, and resilience.)

Even with increasing numbers of consumers installing generating equipment on their own premises, and using the distribution system to access the bulk energy system when on-site generation is not available, it is unlikely that the majority will go entirely "off grid" in the near future. Although many technologies and service offerings are enabling an increasing number of customers to meet larger

portions of their electricity needs with on-site generation, for economic, technical, and regulatory reasons most observers (and the committee) do not anticipate that the dominant customer profile will be self-sufficient and disconnected from the grid during the time frame of interest in this study (i.e., in the next two decades). Moreover, individual self-sufficiency is unfeasible for the majority of the population, and local distribution system planners have to plan to meet the uncertain loads of customers for the foreseeable future.

**Finding:** There is no single organization responsible for mandatory reliability standards in electric distribution systems in the United States. State utility regulators often set standards for the allowable frequency and duration of system and customer outages. In many cases, outages caused by major events are *excluded* when computing reliability metrics.

### Sensing, Communication, and Control in the Distribution System

The technological sophistication, penetration of sensors, deployment of advanced protection devices, communications technologies, computing, and level of automation deployed by distribution utilities vary significantly across the United States. As in the case of transmission systems, distribution networks have been undergoing a transition from analog devices to digital. However, in many distribution systems, it is more difficult to justify large investments in modernization and digital controls, in part owing to factors such as customer density on circuits, circuit configurations, existing performance, and component age. Thus, many distribution systems still operate as they did when built after World War II. However, given the substantial investments (exceeding \$25 billion annually [EEI, 2017]) under way in replacing aging distribution infrastructure, there is an opportunity to enhance the reliability and resilience of the distribution systems through incorporation of advanced technologies, and some distribution utilities have made extensive upgrades.

Protective relays located at distribution substations are used to sense faults, such as a downed wire, and in turn signal the feeder circuit breaker to open. Some feeders have switches that can detect and isolate faults, albeit less frequently (as discussed previously). Distribution laterals that extend from the main feeders have fuses installed that protect the main feeder from faults that occur on the lateral branch. Together, protection devices are critically important for maintaining public safety and for limiting the extent of an outage, in some cases preventing disturbances from cascading higher up in the system.

Each of these devices, relays, switches, and fuses are designed to operate in a coordinated manner. These distribution protection schemes are undergoing a similar analog to the digital transformation occurring on transmission systems. Over the past 20 years, electromechanical relays

<sup>14</sup> Certain energy efficiency measures can function as DERs so long as they are dispatchable, meaning they can be turned on or off when needed by the utility. Other definitions do not emphasize that DERs be dispatchable—for example, FERC's definition at <https://www.ferc.gov/whats-new/comm-meet/2016/111716/E-1.pdf>.

have increasingly been replaced with digital, and now communicating, software-based relays as old equipment reaches end-of-life or when new substations are constructed. Similarly, switches on some feeders have been replaced with more advanced and automated switches when it is cost-effective and justifiable. Protective fuses also have digital communicating alternatives, but these are still largely in demonstration studies to evaluate cost-effectiveness and applicability.

Beginning in the 1990s, many utilities selectively installed SCADA on distribution systems for feeder breakers, mid-point reclosers, and back-tie switches (as well as capacitor bank controls), along with distribution management systems to operate these devices. These first-generation automation systems allowed utilities to operate circuit breakers, switches, and components remotely, which previously required personnel in the field. By sectionalizing circuits in half, these early systems allowed more rapid restoration of the faulted half of the circuit. Such systems have been implemented by many utilities in metropolitan areas where high customer densities enable cost-effective applications.

More recently, a second generation of distribution automation technologies has been adopted. Outage management systems (OMS) that provide greater visibility into distribution circuits and support operators in making restoration decisions have been deployed over the past decade. Some utilities have implemented advanced automation technologies that locate faults, isolate faulted sections, and automatically restore remaining sections to service. Similar to first-generation automation systems, these systems are typically cost-effective only in areas with high customer density per mile of line and on overhead lines with exposure to environmental conditions that reduce reliability and impair restoration.

Although at present these technologies have only been implemented on a fraction of distribution systems across the country, continued deployment of distribution substation SCADA and first- or second-generation automation has the potential to improve the reliability and resilience of the nation's distribution systems, albeit if implemented selectively and as part of a long-term improvement plan. For example, select utilities in areas with significant exposure to environmental threats (e.g., Southern Company in the southeastern United States), or with the need to have greater visibility and control over DERs (e.g., Southern California Edison), have installed or are pursuing advanced automation technologies for automatic reconfiguration of feeders based on outage and load/local generation conditions. However, it is unlikely that these second-generation automation technologies will be deployed in lower-density rural areas or in newer underground systems, as the potential benefits do not typically justify the increased costs.

Compared to transmission systems, which have greater deployment of sensors and therefore provide operators with much better awareness of system behavior and operation, often local distribution utilities only monitor circuit breaker

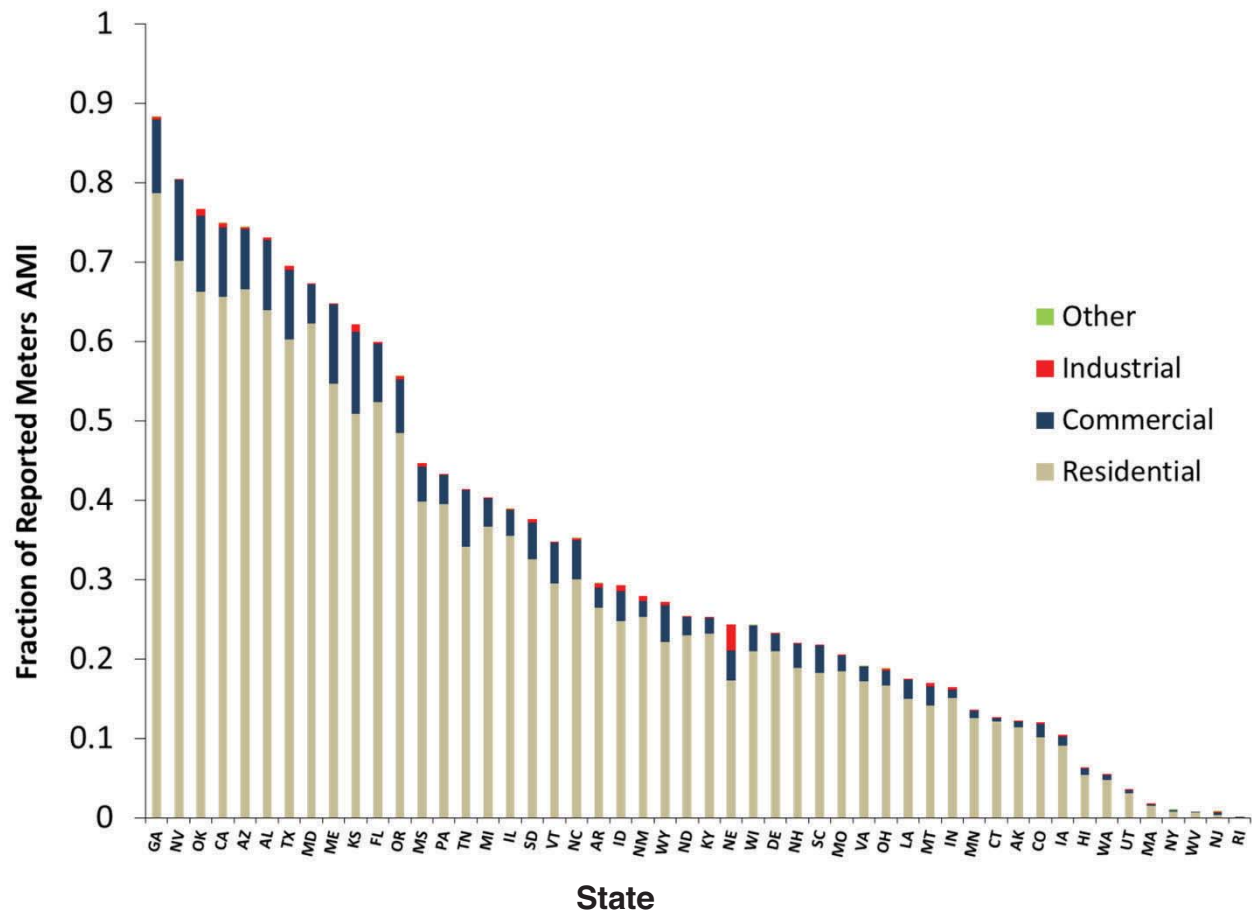
status and measure feeder current and voltage as they leave the substation, and not at other locations on the circuit. However, some utilities installed automation sensing and fault current indicators on feeders themselves, although this level of monitoring is uncommon. Thus, most distribution utilities continue to rely on customer calls to assist in the location of faults. In the most rudimentary cases, utilities without distribution substation SCADA use customer calls to report outages and direct service restoration and repairs.

Utilities have yielded significant benefits from first-generation distribution automation, where cost-effective, but second-generation automation systems are still early in adoption (DOE, 2017b). One utility that adopted second-generation automation with the help of federal demonstration grants reported significant reductions in the severity and duration of outages, as well as economic and operational benefits (Glass, 2016). Of course, actions that increase automation, reliance on software, and communications infrastructure also add complexity and can inadvertently increase a utility's exposure and vulnerability to cyber attack.

Within the past decade, utilities have completed more than 60 million advanced metering infrastructure (AMI, sometimes also called "smart meter") installations across the United States. These investments were greatly accelerated by incentives arising from funding available in the 2008 American Reinvestment and Recovery Act. Figure 2.8 shows the percentage of electric meters with AMI by state. In distribution systems where it has been installed, AMI can provide information to assist in identifying the extent and location of customer outages, as well as the primary benefit of reducing the cost of meter reading. However, the outage data from AMI systems tend to be of poor quality and inconsistent for use in real-time fault identification and initial restoration. This is in part because the messages sent to operators are a "last gasp" from a meter losing power, and often the message itself cannot get back to the operations center as the communications network also loses power (most AMI systems installed are based on radio frequency mesh communications networks). As a result, most AMI systems today are used to validate that electricity service to customers has been restored and for postmortem analyses. More advanced AMI systems, which are available today, have addressed this issue and will be able to support real-time operational restoration and improved communication with customers. Furthermore, to take full advantage of AMI, utilities must make substantial investments in database management and analysis software to utilize the large amount of data flowing back to operators.

Deployment of advanced meters has been met with mixed reactions. Some state regulators remain skeptical of the benefits of AMI or contend that equivalent benefits can be achieved at a lower cost to customers (Reuters, 2010; AEE, 2015; NJBPU, 2017). Some customers have been suspicious of technologies that they view not only as expensive, but also





**FIGURE 2.8** Fraction of customer meters with advanced meters by state in 2015.  
SOURCE: EIA (2016a).

as potentially dangerous for their health<sup>15</sup> and for the security of their private data (Karlin, 2012; Spence et al., 2015). AMI roll-outs in some communities have experienced backlash for these reasons, although other AMI deployments have been much smoother.

Inverters convert the DC signal produced by solar panels or batteries to the AC power used on the distribution system and serve as the interface between many DERs and the distribution system. While the main task of an inverter is as an electric power conversion device, modern technology permits inverters to perform a broader array of ancillary tasks, which can be leveraged in power conditioning to support the grid in various ways (these are sometimes referred to as “Smart Inverters”). Currently, inverters operate with a spectrum of capabilities—for example, some are able to stay connected and ride through disturbances (and in some cases can contribute to solutions), while others automatically disconnect during a disturbance. Interim standards issued by

the Institute of Electrical and Electronics Engineers (IEEE) allow for such “ride through” of disturbances, and FERC now requires this capability. These standards remain under revision (IEEE, 2013).

Currently, relatively few of the inverters installed on the system can provide the local utility with visibility into the power injection of the DER into the grid or the ability to control it when necessary. At some point in the near future, when technical standards catch up with technology, it is possible that inverters will have the capability to communicate with utilities and system operators. This can be further leveraged to enhance system resilience under abnormal situations—for example, by changing inverter settings on the fly for adapting to changing grid conditions. Additional details are provided in the discussions in Chapters 4 and 5.

**Finding:** There is wide variation across the United States in the level of technological sophistication, penetration of sensors, deployment of advanced communications technologies, and level of automation deployed by distribution utilities. Many utilities, particularly in metro areas with overhead infrastructure, have invested significantly in first-generation automation over the past 30 years. Where cost-effective,

<sup>15</sup> While the field strengths are miniscule, the concern is with the possibility of health consequences from exposure to the RF communication associated with the AMI. Similar concerns are expressed by some people about a wide range of RF sources in the world today.

more advanced automation is beginning to be implemented to enhance reliability, resilience, and integration of DERs.

**Finding:** Actions that increase automation and reliance on software and communications infrastructure also add complexity and can inadvertently increase a utility's exposure and vulnerability to cyber attack. This is particularly acute with regard to DER integration.

Keogh and Cody (2013), researchers with the National Association of Regulatory Utility Commissioners (NARUC), explain the following:

[The regulatory] frameworks used to evaluate reliability investments are not perfectly equipped to address investments dealing with these large-scale and historically unprecedented hazards, and some improvements to the frameworks may be needed [p. 1]. . . . Those metrics miss two components: (1) They often undervalue the impact of large-scale events and focus on normal operating conditions; and (2) they price lost load at a flat rate, when in fact the value of lost load compounds the longer it is lost [p. 7]. . . . [M]aking every corner of our utility systems resistant to failure may prove cost-prohibitive, resilience should be selectively applied to the areas that need it most. Existing risk management frameworks can be better deployed to help prioritize where the best investments can be made. A resilience investment may be particularly valuable in the face of high-impact disasters and threats that utility systems have not faced before, like national-scale natural disasters or man-made cyber and physical attacks [p. 1].<sup>16</sup>

Thus, because the existing reliability metrics used to inform regulatory decision making are inadequate for informing resilience investments, continued research is needed to develop analogous metrics for electricity system resilience. Some regulators have begun to consider how resilience objectives should be incorporated by utilities in their jurisdictions, with several prominent examples promising to transform the electric industry today. In response to Superstorm Sandy, for example, New Jersey regulators approved more than \$1 billion in storm-hardening investments for critical substations and building additional distribution circuits for greater redundancy (NJBPU, 2015).

**Finding:** The decisions made by state public utility commissions and the boards of public or customer-owned utilities have significant influence on the reliability, cost, and resilience of distribution systems. The committee agrees with a NARUC analysis that concludes that techniques for guiding

and approving reliability investments are inadequate for resilience.

## METRICS FOR RELIABILITY AND RESILIENCE

### Reliability Metrics Are Relatively Mature and in Widespread Use

Reliability has long been a component of utility planning and operation, and there are many mature metrics to quantify reliability and evaluate potential reliability improvements associated with different grid investments. Reliability metrics are grouped into those applied to generation and transmission systems (e.g., adequacy, loss of load probability) and those for the distribution system, with common examples defined in Box 2.2. Metrics for generation and transmission are used by FERC and NERC, whereas oversight of reliability at the distribution level is left to state regulatory agencies. As previously discussed, ownership and operation of the U.S. electric system is characterized by a mixture of public, private, and cooperative institutions with different incentives and organizational structures, and these different institutions are regulated differently. Thus, different organizations are responsible for maintaining different packages of standards in different locations, some of which can only be attained through collaboration with others.

While reliability metrics are more established and widely used than resilience metrics, there remain many opportunities to improve their formulation and utilization. Although valuable, distribution system metrics that present average values lack details regarding the types of customers experiencing an outage and the severity of individual outage events. Thus, there is a need to increase the granularity of reliability metrics, and the Department of Energy (DOE)-sponsored Grid Modernization Laboratory Consortium (GMLC) is in the process of developing metrics for distribution reliability with greater spatial and temporal resolution (GMLC, 2017). Another critical opportunity for improvement is to better connect reliability metrics to the economic benefits of more reliable service, which requires an understanding of how different customers value reliable electric service.

As society becomes ever more dependent on continuous electricity supply, and the technologies and institutional structures employed to provide that service evolve, it is important to rethink the system's reliability criteria. To the extent that electricity supplies become more distributed, micro-sized local supply communities may take care of their own unique local needs; but to the extent that a significant component of supply is provided over a regional power grid, all users share equally in that bulk supplier's reliability (what is defined as a "public" good by economists) and so some centralized authority is needed to set and enforce the reliability standard for that supply entity. That standard could be based and routinely updated on some systematic estimate of the value of its reliability (and resilience, too).

<sup>16</sup> The authors also explain, "If an investment avoids or minimizes service interruptions in the absence of an extraordinary event, it is just an everyday reliability investment, and the means already exist for utilities and regulators to thoroughly consider it. An important point . . . is that resilient infrastructure does more than one thing well, because a resilience investment needs to pay for itself and create value for ratepayers, even when it is not being used" (Keogh and Cody, 2013, p. 5).



## BOX 2.2

### Common Distribution System Reliability Metrics

#### SAIFI

"System Average Interruption Frequency Index (Sustained Interruptions)—This is defined as the average number of times that a customer is interrupted during a specified time period. It is determined by dividing the total number of customers interrupted in a time period by the average number of customers served. The resulting unit is 'interruptions per customer'" (APPA, 2014).

#### SAIDI

"System Average Interruption Duration Index—This is defined as the average interruption duration for customers served during a specified time period. It is determined by summing the customer minutes off for each interruption during a specified time period and dividing the sum by the average number of customers served during that period. The unit is minutes. This index enables the utility to report how many minutes customers would have been out of service if all customers were out at one time" (APPA, 2014).

#### CAIDI

"Customer Average Interruption Duration Index—This is defined as the average length of an interruption, weighted by the number of customers affected, for customers interrupted during a specific time period. It is calculated by summing the customer minutes off during each interruption in the time period and dividing this sum by the number of customers experiencing one or more sustained interruptions during the time period. The resulting unit is minutes. The index enables utilities to report the average duration of a customer outage for those customers affected" (APPA, 2014).

#### CAIFI

"Customer Average Interruption Frequency Index—The average frequency of sustained interruptions for those customers experiencing sustained interruptions" (APPA, 2014).

#### MAIFI

"Momentary Average Interruption Frequency Index—Total number of momentary customer interruptions (usually less than five minutes) divided by the total number of customers served" (APPA, 2014).

It is important to note that reliability metrics provide only limited insight about resilience. A survey of publicly owned utilities in 2013 indicated that two-thirds of the responding utilities excluded outages caused by major events when calculating their performance on reliability metrics (APPA, 2014).<sup>17</sup> Thus, planning, operational strategies, and technologies used to reduce impacts and expedite recovery from large-area, long-duration outages may have no impact on a utility's performance measured by reliability criteria.

### Development of Metrics for Resilience Lags Behind Those for Reliability

Unlike reliability, there are no generally agreed upon resilience metrics that are used widely today. This is in part because there is not a long history of large-area, long-duration outages that can be analyzed to guide future investments (which is the case for reliability). Nonetheless, the electricity

sector is arguably more advanced in considering and evaluating resilience than other critical infrastructure sectors. There are myriad resilience metrics proposed in research and most remain immature (Willis and Loa, 2015). Some recent analyses have proposed resilience metrics based on concepts like resistance, brittleness, and dependency. Following the resilience processes introduced in Chapter 1, Kwasinski (2016) proposes that resilience is an attribute with four distinct metrics: (1) withstanding capability, (2) recovery speed, (3) preparation/planning capacity, and (4) adaptation capability. A study at Sandia National Laboratories lays out a broad framework for developing resilience metrics, frequently in combinations, and for valuing their respective contributions to overall customer value (SNL, 2014). Furthermore, individual utilities frequently establish their own metrics to guide decision making. For example, the committee was briefed by the Chicago utility Commonwealth Edison on metrics used in selecting optimal locations to site community microgrids,<sup>18</sup> based on a weighted sum of measures of

<sup>17</sup> Also, of the 180 utilities responding to the American Public Power Association survey, 87 percent collected outage data at the system level, 47 percent also collected data at the feeder or circuit level, and 31 percent collected data at the substation level (APPA, 2014).

<sup>18</sup> A microgrid is an energy system consisting of distributed generation, demand management, and other DERs that can connect and disconnect from the bulk power system based on operating conditions.

customer criticality, historical reliability, projected capacity constraints, and measures of substation health.

As part of the GMLC metrics analysis, researchers from multiple national labs proposed a set of resilience metrics, shown in Table 2.2, that build on a resilience analysis process developed as part of the DOE Quadrennial Energy Review. Because many causes of large-area, long-duration outages have a low probability and their impacts are highly uncertain (e.g., based on the types of customers impacted, the exact tract a hurricane follows), the GMLC metrics analysis emphasizes inclusion of statistical measures of uncertainty alongside reporting of resilience metrics and all consequences are estimated as probability distributions.

Development of resilience metrics and methods to defining resilience goals, as well as comparison of alternative strategies for increasing resilience, remains an active area of research, and the committee believes more research and demonstration is required before the electricity sector can reach consensus on a set of appropriate metrics. Metrics often drive decision making. Establishing and building

consensus around metrics is an important prerequisite for comparing resilience enhancement strategies and for evaluating their costs and benefits. Many of the technologies and strategies for increasing the resilience of the electricity system described in the following chapters are expensive, particularly when implemented on a large scale. Without consistent resilience metrics, large amounts of money could be spent with little understanding of actual resilience benefits and with much of this cost passed on to ratepayers.

### Economic Valuation of Resilience

Metrics for resilience should not be selected merely because they can be quantified easily. In deciding what level of resilience is appropriate, it is important at a minimum to estimate how much a lack of electricity system resilience costs individuals and society. Thus in developing resilience metrics, it is essential to be able to link those measures to the value retained or added to society. Furthermore, market responses and/or survey results may provide inadequate measures of resilience since they have attributes of both a private and a public good (many neighbors share the same benefit). Likewise the services provided by most public or private regulated utilities are combinations of pure public and private goods. This is why standards and regulations are important to maintain and restore quality in electricity markets, which are not classical competitive markets with fully rational decision makers (Hirschman, 1970).

Thirty years ago, with most electric supply utilities vertically integrated, the customers knew who to blame for outages. If the overseeing public utility commission (PUC) did not set and enforce adequate reliability standards, the resulting public outcry often resulted in a government response including public pillorying and/or financial penalties assessed against the responsible utility. In some instances of major outages, the outcry extended to elected officials in state or federal government. The principal example is the 2003 blackout that led to EPAct of 2005, granting new authority to FERC to set reliability standards for the bulk power system and to assess penalties for non-compliance.

Developing and enforcing resilience and reliability metrics will become increasingly complicated as technologies and customer preferences evolve alongside changes in public policies regarding equity and environmental goals. The emergence of competitive markets in some areas of the country has altered the institutional structure of the industry, the nature and form of its regulation, and the structure of its financing. So while competition has replaced regulation in some segments of the industry as the means of ensuring reasonable price levels, maintaining the reliability of the whole system has become more complicated with divided responsibility. At the bulk power supply level today, reliability standards are still maintained, but this is often done through market mechanisms that induce sufficient prices for

**TABLE 2.2** Example Resilience Metrics Proposed by the Department of Energy-supported Grid Modernization Laboratory Consortium

Consequence Category	Resilience Metric
<b>Direct</b>	
Electrical service	Cumulative customer-hours of outages
	Cumulative customer energy demand not served
	Average number (or percentage) of customers experience an outage during a specified time period
Critical electrical service	Cumulative critical customer-hours of outages
	Critical customer energy demand not served
	Average number (or percentage) of critical loads that experience an outage
Restoration	Time to recovery
	Cost of recovery
Monetary	Loss of utility revenue
	Cost of grid damages (e.g., repair or replace lines, transformers)
	Cost of recovery
	Avoided outage cost
<b>Indirect</b>	
Community function	Critical services without power (e.g., hospitals, fire stations, police stations)
	Critical services without power for more than N hours (e.g., N> hours or backup fuel requirement)

SOURCE: GMLC (2017).

adequate generation to be built at needed locations, as well as for generation operators to provide operating reserves and to be available to offer those services (provide adequacy), all as overseen by FERC. At the distribution level, state regulation (and public outcry) is primarily relied upon to sustain the reliability to end-use customers.

In the end, reliability and resilience are for the benefit of the customer and society, and all actions, including rules and regulations, need to reflect customer values. Although a consistent principle should be developed for the nation, cost-effective instruments are likely to vary widely. The application of the principle should take into account variations in climate, nature of hazards, socio-economic and demographic patterns, and the nature of customers (industrial, commercial, residential, essential public services, etc.), all of which may lead to different distribution-system configurations (e.g., there are mesh network designs in some densely populated areas, whereas less populated areas have radial distribution system designs).

No rule is effectively implemented without rewards or penalties assigned for adherence. For private goods, if there is truth in labeling and no hidden defects are possible, the market can take care of those incentives. In the case of public goods furnished by a unique provider in each location, assessing penalties for non-compliance can have pernicious repercussions if the service must be sustained. If compliance requires substantial capital investments, arranging financing can be challenging if the entity is under attack by its regulators and its next period's earnings promise to fall because of the fines. If fines are pooled over a wide area of providers in order to support resilience and reliability investments, there is little incentive for the individual utility to provide reliable service. The nature of such problems will change if numerous local microgrids and community-based distribution consortiums become widespread. Furthermore, the shifting of reliability and resilience decisions to the local level also presents serious challenges for financing. One model might be parallel to the U.S. Department of Agriculture Rural Utility Service's (RUS's) funding of rural cooperative electricity suppliers.<sup>19</sup> In the end, regardless of the form of the institution, reliability and resilience begins at home—at the distribution level with the customer.

Because electricity customers value *both* the reliability and resilience of the system, developing metrics and incentives (or disincentives) for utilities based upon resilience and reliability separately is likely to be sub-optimal. It is important that the possibility of trade-offs between resilience and reliability is integrated into metrics, and that the costs of supplying the sum of the measures do not exceed their combined value to customers and to society as a whole (SNL, 2014). At present, such an overarching valuation of

the burgeoning number of reliability and resilience metrics does not exist to aid in the development of reasonable and enforceable standards.

In addition to developing better resilience metrics and using them to monitor and realize better outcomes, knowing much more about what individuals and society are willing and able to pay to avoid the consequences of large-area, long-duration grid failures is an important input to deciding whether and how to upgrade systems to reduce impacts of an outage. Much of what we know is anecdotal from looking backwards at such failures, such as from Katrina, Sandy, or the Northeast blackout of 2003. Most prior quantitative studies have only examined outages of much shorter duration. Willingness and ability to pay may differ substantially based on geography, electric customer class, and socioeconomic status. So work should proceed in parallel to develop better metrics and a better understanding of consumers' and society's willingness to pay.

**Finding:** While reliability metrics are relatively well established and widely used in electricity system planning and operation, the development of agreed-upon metrics for resilience lags significantly behind. Further, since there is currently no common basis for assessing the relative cost-effectiveness of the existing reliability metrics that differ by purpose, integrating the ongoing work on developing resilience metrics may lead to confusion and duplication in their implementation. Thus it may be difficult to evaluate, compare, and justify investments made to improve resilience and to assess progress made in enhancing both the resilience and the overall reliability of the grid.

**Recommendation 2.1:** The Department of Energy should undertake studies designed to assess the value to customers—as a function of key circumstances (e.g., duration, climatic conditions, societal function) and for different customer classes—of assuring the continuation of full and partial (e.g., low amperage and/or periodic rotating) service during large-area, long-duration blackouts.

**Recommendation 2.2:** The Department of Energy should engage the North American Electric Reliability Corporation, the National Association of Regulatory Utility Commissioners, the National Rural Electric Cooperative Association, and the American Public Power Association in a coordinated assessment of the numerous resilience metrics being proposed for transmission and distribution systems and seek to operationalize these metrics within the utility setting. That assessment should focus on how system design, operation, management, organizational actions, and technological advances are affected by those metrics. All metrics should be established so that their cost-effectiveness in bringing added value to the nation can be assessed. Complementarities between metrics should be identified, and double counting of their effects should be avoided.

<sup>19</sup> The RUS provides loans and loan guarantees to help finance construction and operation of electric distribution and transmission systems (among other things) in rural areas. Electric cooperatives (and other utilities) may receive such financial support from the RUS (USDA, 2016).

## NEAR-TERM DRIVERS OF CHANGE AND ASSOCIATED CHALLENGES AND OPPORTUNITIES FOR RESILIENCE

As described previously, significant transitions are currently under way in the power system and its associated institutions. Some changes result from market fundamentals including changing customer preferences, others from an array of state and federal policies, and yet others from technological innovations that offer both opportunities and new challenges for the grid, especially in terms of resilience. The future electric system will have a more complex array of central-station power plants on the bulk power system, as well as DERs behind customers' meters or otherwise attached to the local distribution system. Many more players will use technologies and applications that can expose the grid to greater risk of cyber attack. These changes may both facilitate and complicate the development of greater reliability and resilience. Starting with a description of these various trends that are affecting the grid, this section discusses some of the implications of those trends for the resilience challenges its owners, operators, and users will increasingly face in the years ahead.

### Power Market Fundamentals

The nation's "shale gas revolution" began a decade ago and has contributed to a changing generation mix in many parts of the United States, particularly where coal-fired or nuclear generation have been major players. In combination with a decade of flat electricity demand (EIA, 2016b), loss of cost advantages for coal (Tierney, 2016a), declining costs for small-scale and utility-scale wind and solar generating technologies (Lazard, 2015), and controls on emissions of mercury and other toxic air pollutants, this has contributed to retirements of 49.3 gigawatts (GW) of coal-generating capacity since the year 2000 (EIA, 2016c). Most of these plants were older, relatively inefficient, and without modern pollution controls. Because of competition from low-cost natural gas and the high costs of plant life extensions, several nuclear plants have been retired in recent years with others facing premature closure (BNEF, 2016).

The vast majority (91 percent) of the 403 GW of generating capacity added since 2000 has been at gas-fired generating units (281 GW), as well as wind and solar installations (together, 87 GW) (EIA, 2016d). In 2016 alone, utility-scale wind, solar, and gas-fired capacity amounted to 93 percent of total generating capacity additions (EIA, 2016d). Another 2 GW of distributed solar capacity was added in 2015, which is the most recent year reported by EIA (EIA, 2016e). The changing electric generating mix is introducing new challenges for grid operators, who must keep generation and consumption balanced with a decreasing amount of baseload coal and nuclear assets and an increasing share of intermittent, non-dispatchable generating resources.

DERs differ from the large central generators that traditionally form the backbone of the grid in that DERs are much smaller, located closer to consumers, and often controlled in a decentralized fashion by local users themselves. The shift to DERs comes as a result of changes in technology, customer preference, and policy. Technologically, numerous new power supply, response, and control systems are emerging. At the same time, federal and state regulators, as well as others, are pushing for the adoption of DERs with a variety of goals that are described further in Box 2.3 and in the following section. As with almost any change in technology, these driving forces interact in many complex ways. Some of the changes in technology are purely exogenous, but most are responding at least partly to policy signals. These forces also interact with consumer preferences, as is typically observed with changes in other technologies. New technologies for local supply and power conditioning have seen early adoption by users who have a particularly strong preference for reliable power, such as hospitals and server farms.

### Federal and State Policy Drivers

The federal government and most states have been active in adopting policies aimed at promoting the introduction of efficient and renewable energy technologies, controlling emissions associated with power generation, and fostering innovation and grid modernization. These policies, many of which are mentioned in Box 2.3, have impacted both the bulk power and local distribution systems. Importantly, but with notable exceptions, federal and state policies that have encouraged development of advanced technologies and DERs have been motivated by considerations of economic development, environmental impacts, or clean-energy goals, rather than by concerns for resilience and reliability.

While many of these federal and state policies have been directed toward regulated utilities, many have encouraged non-utility entrants to make investments, operate programs, and bring new technologies to the marketplace. Today, many of the devices (e.g., central-station power plants, rooftop solar installations and their accompanying smart inverters) attached to the grid are owned by third parties. There are many more actors affecting the operations of the grid, and grid operators and others need to take into account a wide variety of facilities and resources as they assure the operational reliability and security of the grid.

To gain a better appreciation of the state of DER and microgrid adoption in jurisdictions across the country, the committee sent a questionnaire to public utility commissions in all 50 states and the District of Columbia and received nearly 25 responses. The questionnaire sought anecdotal information about variations in deployment of smart meters, distribution automation, organized DR programs, CHP facilities, and questions regarding legal constraints on microgrids across the country. Answers called attention to wide differences in adoption of these technologies and views on their



### **BOX 2.3**

#### **Federal and State Policy Drivers of Change in the Electric System**

##### **Federal Drivers**

- Encouraged the development of alternative energy produced by non-utility generation (e.g., PURPA in 1978);
- Promoted competition in wholesale electricity markets (e.g., through the EPActs of 1992 and 2005);
- Mandated the introduction of increasingly efficient electric appliances into the marketplace;
- Supported utilities' investments in advanced meters and other technologies (e.g., through the American Recovery and Reinvestment Act of 2009);
- Required mandatory reliability standards and authorized incentive rate of returns on some transmission investments on the bulk power system (both under the EPAct of 2008);
- Introduced investment and production tax credits for renewable electricity;
- Adopted new regulations under the decades-old Clean Air Act to control air toxic and carbon-dioxide emissions from existing fossil-fuel generators; and
- Standardized small generator interconnection procedures.

##### **State and Local Drivers**

- Opened retail commodity markets to competition and third-party innovation (see Figure 2.6);
- Encouraged the development and adoption of renewable resources (DSIRE, 2016a, 2016b, 2016c);
- Developed state tax incentives for energy efficiency and renewable energy (DOE, 2016b; DSIRE, 2016d);
- Installed advanced metering devices and microgrids in New York and California, for example (Tierney, 2016b);
- Developed rate designs (such as net metering<sup>a</sup> tariffs or time-of-use rates) to encourage DER adoption;
- Implemented energy efficient appliances, green buildings, and other measures to increase the efficiency of energy use (ACEEE, 2012; Alliance to Save Energy, 2013);
- Promoted adoption of electric vehicles and installation of the charging infrastructure to support them (Plug-in America, 2016); and
- Adopted technologies to control carbon emissions from power plants (RGGI, 2016; CARB, 2014).

<sup>a</sup> Net metering is a billing arrangement in which a customer with distributed generation receives credit for the energy he/she provides to the grid, sometimes at full retail rates or a fraction thereof.

potential to increase system reliability and resilience across the United States, as summarized in Box 2.4. Although not quantitative and not used to make any comparative statements, the answers received by the committee broadly align with previous studies done by FERC (2016b) and stakeholder groups (Gridwise Alliance, 2016).

#### **Changing Time Scales for Grid Operators**

Along with the changes to the fundamentals of the generation mix, the electricity power system is undergoing changes to the time scales for operations, especially in the area of power markets for restructured utilities. The future will see continued shortening of time scales for grid operations: data on system conditions come in on time scales under a second, and the dispatch of resources and market settlements happens every 5 minutes. The requirements for such rapid dispatch and analysis have impacted the tools used to manage the system, causing the energy management systems within RTOs to be custom built. The operational concerns of the collapsing time frames and the human interface are real. Though

the resilience impacts of these changes are complex, these challenges motivated the committee to recommend research on improvements to system operator control rooms and the application of artificial intelligence to power system monitoring and control within Chapter 4. These concerns also help motivate overarching recommendations to improve the security and resilience of the cyber monitoring and controls systems within Chapter 7.

#### **Industry-Structure and Business-Model Transitions**

There are new industry structure and business model issues that are also in transition, with uncertainty about which direction they will take in the future (NASEM, 2016; MIT, 2016). Competitive forces, often stimulated by actions of federal and state legislatures and regulators, have prompted an array of new actors (e.g., non-utility generating companies and independent non-utility transmission companies), new institutions (e.g., RTOs and ISOs), and new issues subject to FERC regulation in wholesale electricity markets and the bulk power system. Most of these institutional changes have

### BOX 2.4

#### Example Comments to the Committee on Distributed Energy Resource and Microgrid Deployments Across the United States

Staff of the Pennsylvania PUC noted that “there are no utility-owned or operated microgrids in Pennsylvania at this time. However, there are some campus and commercial test beds, especially in the Philadelphia and Pittsburgh areas. . . . The Pennsylvania PUC encourages distribution utilities to make use of advancing technologies and support CHP projects. Smart meters are mandated for all large electric distribution companies.”

The New Jersey Board of Public Utilities was the only state utility regulatory organization that indicated a microgrid was able to sell electricity directly to “one customer across one right-of-way,” as well as being able to sell power into the wholesale market operated by the RTO PJM.

The Georgia Public Service Commission (PSC) described major investments made by Southern Company in advanced metering and distribution automation: “The resulting smart grid network will greatly improve reliability for Southern Company customers. . . . Georgia Power reports its reliability statistics (SAIDI, SAIFI) annually since 2003. Since the installation of the smart grid equipment, these metrics have trended downward.”

According to staff of the Illinois Commerce Commission (ICC), “The Illinois General Assembly has enacted laws, and the ICC has adopted ratemaking policies that support and encourage the development and deployment of new technologies and facilities. Utilities report that their actions combined with customers’ responses to programs tied to new technologies result in reliability and resiliency improvements.”

In Kansas, the state Corporation Commission staff responded, “So long as these technologies are dispatchable by the incumbent utility, staff views them as supportive of system reliability and resiliency.”

Staff of the North Carolina Utility Commission informed the committee, “The Commission encourages utility consideration and deployment of cost-effective new technologies that would improve the reliability and resiliency of the electric grid. The utilities are required to address these technologies in their integrated resource plans and smart grid technology plans filed with, and reviewed by, the commission.”

The Montana PSC staff indicated, “The PSC supports regulated utilities to engage in pilot projects and studies to gain insight into potential benefits of [advanced DER] technologies.” One utility in their jurisdiction is “currently engaged in a smart meter pilot project with some use of distribution automation.”

Staff of the Idaho PUC told the committee that advanced DERs and automation technologies “improve outage control, system monitoring, and reduction in system peaks to reduce overall costs.”

Staff from the Iowa Utilities Board indicated, “With market refinements, these technologies enable the utilities to flatten the demand (load) curve by passing appropriate price signals. Proper price signals result in build-up of generation only as needed and thus improve system reliability and resiliency.”

Staff of the Delaware PSC noted that there are “a few installations where [distribution] feeders are automatically reconfigured upon loss of service. These installations are limited to critical service customers such as sewage pumping or water pumping stations.” Staff went on to say that “reliability and resiliency need to be balanced with the costs that ratepayers will incur with the new technologies.”

In Wisconsin, PSC staff explained that they have “not taken any formal action related to the ability of these technologies to improve grid reliability and resiliency. . . . Wisconsin utilities typically have good reliability indices and high customer satisfaction, and [advanced DER technologies] do not necessarily result in improvements in SAIFI, SAIDI, and CAIDI, so it is difficult to measure how these technologies directly affect reliability.”

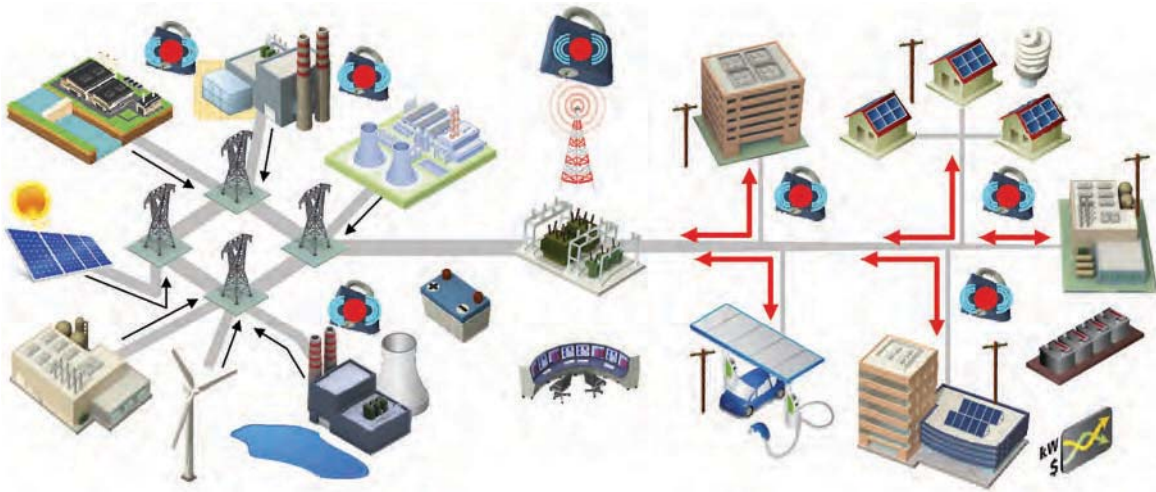
The Regulatory Commission of Alaska observed, “The electricity infrastructure in Alaska differs from that in the lower 48 states in that Alaskans are not linked to large, interconnected grids. . . . Most of the state’s rural communities have no grid access and rely on community electric utilities to provide service via diesel generators.”

already occurred. Unlike the bulk power system that has undergone significant restructuring and regulatory reform over the past decade, the structure and regulation of electric distribution systems has, until recently, experienced much less change. Thus, the committee considers that the largest changes to the structure of the electricity system in the future will occur within the distribution side of the system.

At the distribution-system and retail electric level, the relatively rapid emergence of DERs has accelerated pressure on regulators, utilities, and other stakeholders to address aspects of the traditional utility business model, which has supported grid investments largely through rates that recover significant

quantities of utilities’ fixed costs through usage-based charges. All else equal, as new small-scale technologies generate power from customers’ premises and inject it into the grid (Figure 2.9), causing revenues from volumetric rates charged to customers to drop, utilities and others have begun to look for regulatory frameworks and new rate designs that assure that all customers pay their fair share of the costs of maintaining a reliable and resilient grid. The approaches under discussion across the country for the future roles of the local distribution utility include the “enhanced status quo,” the “network service provider,” the “market enabler,” and the “solutions integrator” (De Martini and Kristov, 2015; State





**FIGURE 2.9** Schematic of possible electric system configurations and interactions in the future.  
SOURCE: EPRI (2011).

of New York, 2014; Tierney, 2016b; TCR, 2016). These new business models are relevant for resilience considerations in light of the fact that each poses different implications for the entity(ies) responsible for supporting resilience on the grid:

- *Enhanced Status Quo.* In this model, utilities will continue to manage their generation and/or delivery infrastructure to supply power to customers as today. At the same time, utilities will continue to invest in replacing aging infrastructure and advanced grid technologies to improve system reliability and resilience under traditional regulatory cost-of-service, ratemaking, and cost-recovery models (including revenue decoupling, in which utility cost recovery is delinked from volumetric electricity sales).
- *Network Service Provider.* As a more distributed energy future unfolds, the distribution system becomes a platform for enabling DERs to provide services to the wholesale market and as “non-wires alternatives” (so called because targeted installation of DERs can defer the need for transmission expansion). This model expands the role and value of the distribution system. This is accomplished by providing open access distribution services enabled by advanced technologies to allow the integration of high levels of DERs. Distribution services are based on network access fees comprised of demand charge and fixed charge components. Financial incentives for operational performance (e.g., for reliability and interconnections) and earnings mechanisms on DER non-wires grid services are employed. Otherwise, the traditional regulatory and utility economic model remains.
- *Market Enabler.* This model focuses on expanding the role of the utility distribution operations to become the distribution system (or market) operator (DSO).

This “total DSO” (De Martini and Kristov, 2015) has responsibility for balancing demand and supply as well as distribution network reliability for a distribution area to an interchange point with the bulk power system operator. In this role, the DSO provides a single aggregated interface with the ISO/RTO, requiring the DSO to optimally dispatch DERs within its area. Traditional regulatory and utility economic models apply, along with the incentives above and market-based pricing for optional competitive services.

- *Solutions Integrator.* This model focuses on developing customer DER assets alongside other energy services, such as power and natural gas commodity supply, energy information services, and energy efficiency retrofits. In this model, utilities provide turn-key or selected engineering, procurement and construction services to support reliability, enhancement projects, customer high-voltage infrastructure, microgrid, and DER implementation. Services may also include customized engineering and operational consulting as well as emissions management and equipment condition assessment to ensure safety and reliability.

A critical factor in the transitions of the electricity sector is that continuing reductions in the cost and accelerating deployment of DERs is leading to a new class of customer that is both an electricity consumer and producer (“Prosumer”). There are now large and small prosumers who are increasingly interested in managing various aspects of their own electricity usage and supply. This is also enabling greater customer choice for installing select DER technologies to satisfy individual customer requirements associated with reliability, redundancy, and power quality. Whereas most backup power requirements in the past relied on diesel generators, numerous other DER technologies can supplant

or even replace the diesel generator as a backup power option. However, DERs have complex impacts on resilience, which are discussed in the following sections and throughout the report.

### **Distributed Energy Resources and the Distribution and Transmission Systems**

DERs can provide benefits not only to the customers that employ them directly, but also to the broader transmission and distribution system. For example, DERs may help avoid or defer the need for new generation, transmission, or distribution infrastructure to address congestion, localized reliability, or resilience issues. The value of DERs for reliability, efficiency, and resilience depends upon their location and their particular attributes (e.g., their durability, their ability to be controlled, their availability when needed, the times of day when they reduce net load to the grid). Absent effective planning, DERs can also impose costs on the electricity system—for example, through equipment upgrades necessary to handle generation on distribution circuits, sub-optimal DER placement that contributes to congestion as opposed to alleviating it, and incomplete or inefficient sharing of information across the distribution-transmission interface.

This is particularly true at the distribution-system level, but also for interactions with the transmission grid. On the planning side, DERs can interact with the transmission system in several ways. First, behind-the-meter DERs complicate regional load forecasting, the process used to predict customer electricity demand at least 10 years into the future. Transmission system planners design the high-voltage system to meet forecasted demand. DERs behind the meter that provide energy to their owners have the potential to decrease load forecasts by the local retail utilities, which may account for DERs in their forecasting. Bulk power system planners may not be aware of DERs, and their load forecasts may not reflect the locations and types of DERs appearing or expected to appear on the system (NERC, 2016b).<sup>20</sup>

DERs can also be used in transmission-system planning processes to address specific system needs identified through modeling that informs planning. If a planned generating unit retirement or predicted demand increase may lead to a localized reliability issue, DERs could be employed to address that issue in lieu of a more traditional solution like a substation upgrade or new transmission line. Several legal, operational, and institutional barriers to employing DERs as transmission-system solutions exist, but the potential is real.<sup>21</sup> The use of DERs to address transmission-system

limitations may also increase resilience in that the resources are more readily available after an outage or disturbance that could knock out a substation or transmission line for significant periods of time.

On the market design and operations side, DERs also have implications for the transmission system. In addition to potentially reducing the capacity-procurement needs of a region, DERs are legally able to participate in wholesale energy, capacity, and ancillary service markets. These centralized markets exist only within the RTO and ISO regions shown in Figure 2.5; the rest of the transmission-owning utilities rely on bilateral contracting or self-supply to meet their electricity needs.<sup>22</sup> Some DERs have made progress in wholesale market participation. In PJM, for example, demand response resources participating in the wholesale market totaled more than 9,800 MW, with resources positioned at more than 17,000 locations across the PJM footprint (McAnany, 2017).

On both the transmission planning and wholesale market sides, a lack of operational awareness and coordination between distribution utilities (or, in the future, “distribution system operators”) and transmission-owning utilities, or the RTOs or ISOs operating the transmission system and wholesale power dispatch, serve as additional barriers to capturing the full potential value of DERs to the electric system. DER owners must understand what planning and market opportunities exist at both the distribution and transmission levels, and utilities and market operators must understand when resources are available for their use and when they are otherwise committed to provide grid services that render them unavailable for other uses.

**Finding:** The value of DERs for reliability, efficiency, and resilience depends upon their location, their attributes, the planning process behind their installation, and the legal and regulatory environment in which they are operated. While they can contribute to reliability and resilience, absent effective planning and an appropriate regulatory environment, DERs can also impose vulnerabilities and costs on the distribution system.

### **Other Technology Developments**

Other new and emerging technologies may have important impacts on the structure and operation of the power system, including lower cost batteries as well as falling cost and growing capabilities of power electronics. Energy storage in the distribution system and on the customer side of the meter is a relatively new phenomenon. Some distributed energy storage (DES) is provided by thermal systems such as

<sup>20</sup> For example, the RTO that covers 13 Mid-Atlantic states and the District of Columbia, called PJM, was able to decrease its load forecast by 6,000 MW for 2020 by incorporating the energy efficiency and distributed solar that exists or is planned to come online between now and then (PJM, 2016).

<sup>21</sup> See Southern California Edison and Consolidated Edison projects discussed in Tierney (2016b).

<sup>22</sup> One notable exception is the recent development of an Energy Imbalance Market (EIM) administered by the CAISO, with participation by a growing number of utility systems in the Western grid. As of 2017, several electric utilities in Arizona, California, Idaho, Nevada, Oregon, Utah, and Wyoming had joined or are planning to join the EIM (CAISO, 2017).

hot water heaters. Other DES technologies involve chemical (e.g., battery) solutions. There is large variation in projected battery costs, potentially declining from today's levels of about \$600/kWh for whole battery systems to the range of \$200–\$300/kWh by the early 2020s. Lower cost batteries are providing interesting opportunities. Customers are installing on-site battery systems behind the meter in service areas with high charges for peak power consumption to shift their usage to off-peak periods. In general, energy storage has the potential to enable the electric system to become more efficient while enabling customer-side energy management (Navigant Research, 2013).

Over the next 20 years, customers will likely have greater technological opportunities to go entirely off grid, satisfying their electricity requirements with a combination of on-site generation and storage technologies. Customers capable of investing in such packages of technologies (or purchasing such services from the utility or a third party) may be able to take personal responsibility for their own resilient electric service. Although the committee believes the share of total customers taking advantage of such approaches will be limited, trends in grid defection and the technologies that could enable it should be closely monitored. Broader impacts on social equity will also warrant attention.

The controllability of DERs is enabled by low-cost computing and communications technologies. The internet of things and edge computing have progressed to the point where the capability to control DERs at low cost has become much more practicable, with significant advances even over the past few years. There is also significant experience among a number of utilities and third-party aggregators implementing and operating “smart grid” technologies that include operation of distributed generation, storage, and demand response. Fundamentally, the computing and communications technologies are not the limiting factor for adopting these control strategies, although they will require increasing sophistication and resolution in the monitoring and control systems used at the individual feeder and substation scale to understand and optimize circuit health and behavior.

Most organizations that have employed various DER strategies on a large scale have discovered that the need for “big data” analytics and other strategies to optimize the operation and control of these distributed assets is nascent, and more effort is needed to further develop the algorithms to enhance system operations and resilience by managing DER deployment. This is particularly true during off-normal conditions where the DER might be providing emergency backup power to support system restoration. Finally, these DER assets will necessarily need to interact with each other seamlessly, including during normal and off-normal or emergency situations, and not create or exacerbate any adverse conditions. These include but are not limited to hazards to utility workers and the public, equipment damage, and sub-optimal operation of the remaining electrical assets.

## Interdependencies Between the Electric and Natural Gas Infrastructure

One outcome of the trends under way in the electric system is the industry's overall reliance on natural gas to fuel power generation, which increases the electric system's reliability on conditions in the gas industry. This has potential implications for the resilience of the grid. The conventional wisdom is that the electric industry will become even more dependent upon natural gas than it has in recent years, and the natural gas industry looks to a future in which significant growth in demand depends upon developments in the power sector. For the electric system to become more reliable and resilient, attention must be paid to assure robust systems and practices across the two industries.

For many years, these two systems developed on largely different paths, from physical, economic, engineering, institutional, industrial-organizational, and regulatory perspectives. Both industries evolved with some degree of vertical integration and with aspects of each industry's value chain regulated as monopolies by federal and/or state governments. The interconnected networks of each industry expanded over larger and larger geographic footprints. Recently, both systems have undergone eras of significant industry restructuring, with new players emerging as functions became unbundled and as competition entered into different parts of the business.

Today, however, each industry has its own set of cost structures, operating protocols and standards, commercial instruments, and pricing arrangements. Further, while the electric system operates as a network, following laws of physics on an interconnected grid rather than ownership or contract paths, the natural gas system is not a network industry. Individual companies own segments of the pipeline system, and users contract for access to and use of specific facilities. These changes also have occurred in parallel with dynamic developments in real-time, internet-based communications systems, complicating the interdependencies and allowing opportunities for new arrangements and solutions.

Today, natural gas supply still tends to move long distances from production sources to users' sites, typically to locations where there is little to no storage close to or on the end-user's property. This means that from an operational point of view, gas resources need to move “just in time” (i.e., they are used as they are delivered) to the end user through pipelines. During certain seasons and times of the day, many of these pathways—for example, those serving the Mid-Atlantic and Northeast regions—can become quite congested with firm gas deliveries, recognizing that gas injections at the production locations are intended to balance withdrawals of gas from the delivery system while taking in to account a variety of operational issues along the pathway from production to use. (“Just in time” delivery, however, sits within a context in which natural gas moves between 15–20 miles per hour on the interstate pipeline system, while



electric system operations occur at the sub-minute and multi-minute time frame.) Further, the growth in the power sector's use of natural gas has not been accompanied in all relevant regions by expansions in pipeline capacity or increases in the efficiency of existing gas delivery infrastructure. Without change in some of the key features in current business models for competitive generators or in market rules, that situation is not expected to change dramatically in the near term, making it difficult to drive investment in pipeline/storage infrastructure based on demand from the electricity sector. (In some regions such as New England, however, changes in market rules have led many gas-fired generators to invest in dual-fuel [oil/natural gas] capability with on-site storage of oil as a lower-cost means to assure the ability to operate during periods when delivery of natural gas over pipelines is otherwise constrained.)

Regulatory issues at the intersection of gas and electric markets are complicated. While FERC may have responsibility for a broad set of policy issues on electric/gas integration issues, and NERC is evaluating the interdependencies from an operational and planning perspective, the states have strong interests and, in some cases, regulatory responsibilities that can affect market participants' behaviors as well. Importantly, the structure of the natural gas production and delivery system in the United States does not have the same reliability requirements as now exist in the electric industry, and parts of that supply chain (e.g., production of natural gas) are effectively outside of FERC's regulatory jurisdiction.

The electric and gas systems are already experiencing strains at their intersection. To date, integration issues related to increased gas-fired generation have caused rotating power outages in the Electric Reliability Council of Texas during the big freeze of 2011. And, owing to winter gas shortages and extreme cold weather, natural gas was either unavailable or priced too high for generators in PJM and the New York ISO during the polar vortex of 2014 (see Box 4.2 for a description of these events). In some regions, for example, generators need to commit to move gas volumes before knowing whether their offers into the RTO's daily power markets have been accepted; conversely, generators need to offer prices into such energy markets without fully knowing the price and/or availability of their natural gas. There are other instances where gas customers that have contracted for firm gas supply and transportation service face potential (or real) curtailments as operational conditions change upstream and downstream. Tensions are visible across the business models of different players in the two industries and in the market rules in different regions. Further, there are different attitudes across the two industries regarding the urgency of anticipated changes in natural gas supply associated with growing use for electricity generation—specifically, the need for increased total supply and for that supply to be more nimble. It is difficult enough to introduce change into a single industry, where there may be players who perceive themselves as winning or losing from different options for

resolving small and large issues. It will undoubtedly be even more difficult to introduce sensible but meaningful changes affecting market participants in two industries.

Decisions by myriad market actors and institutions do not typically reflect coordinated information about the performance of systems either across industry segments (e.g., across the electric and gas industries) or within industry supply chains (e.g., from production sources across interstate transmission systems). In the context of the events that occur in one or more parts of the industries' systems, this absence of coordination mechanism may make some aspects of resilience—preparing for outages so as to limit their impact, sustaining service during an outage, and/or in restoring the systems to normal operations after the event—difficult to realize.

**Finding:** The electric industry has become highly dependent upon natural gas, and the natural gas industry looks to a future in which significant growth in demand depends upon developments in the electricity sector. For the electric system to become more reliable and resilient, attention must be paid to assuring the availability of adequate natural gas resources at all periods of time, including through investment in natural gas infrastructure (e.g., contractual arrangements and siting and construction of pipelines or storage), where it is economical to do so, fuel diversity for electric generators and natural gas compressors, and the alignment of planning and operating practices across the two industries.

### Emerging Electric Grid Jurisdictional Challenges

Historically, and despite the state-to-state and regional variations in grid regulation around the country, FERC, the states, and regulated utilities have operated within relatively clear jurisdictional boundaries. In an electric grid consisting predominantly of large and dispatchable central station power plants, it was clear that FERC had jurisdiction over wholesale electricity rates and interstate transmission, whereas states had regulatory authority over retail sales and delivery over local transmission and distribution systems into our homes, businesses, and industrial facilities. Power on the system generally flowed in one direction, from the generator all the way to the end-use customers.

Over the past decade, however, the increasing penetrations of DERs and smart grid technology that are relevant for resilience have begun to change the very way the grid operates (see Figures 2.1 and 2.9). The grid is increasingly an interconnected web rather than a straightforward series of one-way pathways. However, the federal, state, and other legal constructs dictating the role of DERs on distribution and transmission systems are in active review by FERC and states in the relevant regions. Although this is a constructive response, there remain many jurisdictional ambiguities, policy mismatches, and an inability to maximize the potential value of technological change toward grid reliability and

resilience. The emerging relationships between DERs and the transmission and distribution systems have greatly outpaced the laws and regulations that govern their interactions. The 80-year-old FPA never contemplated the modern and complex system that exists today. As a result, the relatively clear boundary between state and federal authority over the electric system has blurred to some extent, causing uncertainty, if not confusion, among policy makers and energy industry participants. Recent legal challenges taken up to the Supreme Court have begun to sort through aspects of unresolved jurisdictional questions, but several questions remain.<sup>23</sup>

Jurisdictional issues are also emerging within the distribution and transmission systems themselves. On the distribution system side, regulations typically assume one-directional power flow and fail to contemplate most DERs, including microgrids. From a resilience perspective, microgrids are a particularly interesting development—but they are not without legal uncertainties. Most state regulations obligate utilities to provide distribution service to all customers within their territories. With that obligation often comes the right to be the exclusive distribution provider. Microgrids that would connect buildings or a broader area technically involve their own distribution service and so, in many cases, are prohibited by existing utility regulations.

On the transmission system, the FPA itself remains a barrier to increased DER participation. For example, in the regional system planning processes, the FPA allows for transmission owners to allocate and recover the costs of new transmission investment except for non-wires alternatives, which includes DERs that are traditionally regulated by the states. As noted, the relationship among emerging technologies, evolving business models, and outdated laws and regulations that dictate authority over electric grid activities are stressed by the rapidly changing composition of resources and services involved with the delivery of energy, resulting

in significant uncertainty. This, in turn, creates challenges for resilience planning.

**Finding:** Any new local, state, or federal programs, regulations, or laws designed to increase grid resilience will have to navigate a labyrinth of existing state and federal laws (some of which are out of date) that shape the incentives (or disincentives) for undertaking investments and actions aimed at enhancing resilience. This creates challenges for resilience planning, especially in light of the essential role of electricity in providing critical services and powering the economy.

## LONGER-TERM DRIVERS OF CHANGE AND ASSOCIATED CHALLENGES AND OPPORTUNITIES FOR RESILIENCE

There is, of course, no way to reliably predict what the power system will look like in 30 to 50 years. However, it is possible to identify a variety of developments that could shape that future and then seek strategies that will be robust across that range of possibilities. To that end, here the committee identifies and discusses a variety of factors that might shape the future evolution of the system. Planning for grid resilience needs to take into account the expectation that the grid and its various institutions, technological features, legal structure, and economics will change—and in ways unknown today.

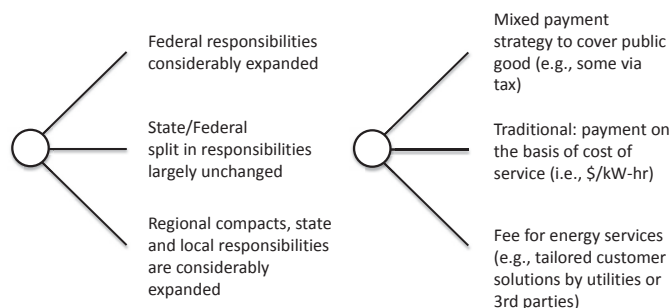
### The Nature and Scope of the Future Regulatory Environment

Recent years have witnessed a dramatic shift in the structure and regulatory environment in which the high-voltage transmission system operates. A similar transformation has not yet occurred at the level of the distribution system. Whether such a transformation will occur, and what form it might take, will likely have profound effects on the future evolution of the system. Will federal authority be expanded to include a larger role at the level of the distribution system (Figure 2.10), as could occur, for example, where customers with on-site generation sell surplus back into the grid and thus set up the possibility of federal jurisdiction where such injections of power were considered sales for resale? Many states would likely oppose such an expansion, in a continuing tension between state and federal oversight seen in previous legislation including various provisions of PURPA and EPCAct 2005.<sup>24</sup> The latter specifies the following:

Each electric utility shall make available, upon request, interconnection service to any electric consumer that the electric utility serves. For purposes of this paragraph, the term “interconnection service” means service to an electric consumer under which an on-site generating facility on the consumer’s premises shall be connected to the local distribution facilities. Interconnection services shall be offered based

<sup>23</sup> These recent cases have clarified a few different jurisdictional principles: First, one Supreme Court decision called *EPSCA v. FERC* determined that FERC has the authority to regulate DER participation in wholesale markets. This authority means that, under certain circumstances, states and the federal government will both have the ability to regulate DERs in the performance of different activities. Second, another high court decision (known as *Hughes v. Talen Energy Marketing, LLC*) recognized that states have the authority to engage in their own preferred resource procurement efforts, but that they cannot cross a line that would invade FERC’s exclusive authority to set wholesale energy rates. The *Hughes* decision has fewer direct implications for DERs that may be procured for resilience purposes than it does for supply-side generating resources like wind, solar, or natural gas power plants, but it is nonetheless important to keep in mind in resilience program design. Third, a Supreme Court case called *Oneok v. Learjet*, considering the Natural Gas Act, emphasized that the ability of the federal government to regulate one particular area does not necessarily preclude state regulation in the same area. Other challenges around the ability of states and the federal government to regulate certain aspects of grid activities that have implications for DERs are working their way through federal courts. Although the mentioned cases have provided certainty in some respects, a general climate of uncertainty exists in states’ attempts to design new DER-centered regulations and programs.

<sup>24</sup> For example, PURPA’s Sections 1251, 1252, and 1254, and section 1254 of EPCAct 2005.



**FIGURE 2.10** Different ways in which the nature and scope of the future regulatory environment might evolve.

upon the standards developed by the Institute of Electrical and Electronics Engineers: IEEE Standard 1547 for Interconnecting Distributed Resources with Electric Power Systems, as they may be amended from time to time. In addition, agreements and procedures shall be established whereby the services offered shall promote current best practices of interconnection for distributed generation, including but not limited to practices stipulated in model codes adopted by associations of state regulatory agencies. All such agreements and procedures shall be just and reasonable and not unduly discriminatory or preferential.

While the legal justification under which federal jurisdiction might be further expanded is unclear, there is certainly a possibility that such justification might evolve over time.

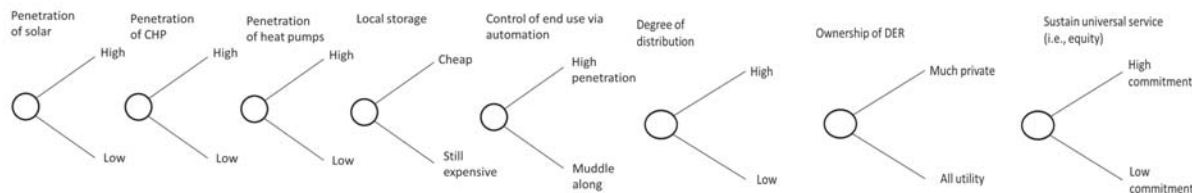
There is of course also the possibility that in some domains, local, state, or even regional regulatory responsibilities might be expanded. If larger differences develop among regulatory structures in different parts of the country, this could present a variety of complications. As pressure grows to adopt more innovative strategies to address resilience issues that impact large areas of interconnected systems, states and regions may decide they need to adopt more innovative approaches.

The possibility of greater grid defection by customers may result in those customers providing their own electricity, entirely removed from federal and state rate jurisdiction altogether. It is likely that this would occur only in situations

where the customer disconnects entirely from the grid. In such instances, states may have to address the terms and conditions under which customers may exit from or reenter the local distribution to assure (among other things) that legacy costs associated with utilities' planning to provide service to those customers are addressed, according to traditional cost-incurrence and equity principles of utility regulation.

### Penetration and Characteristics of Distributed Energy Resources

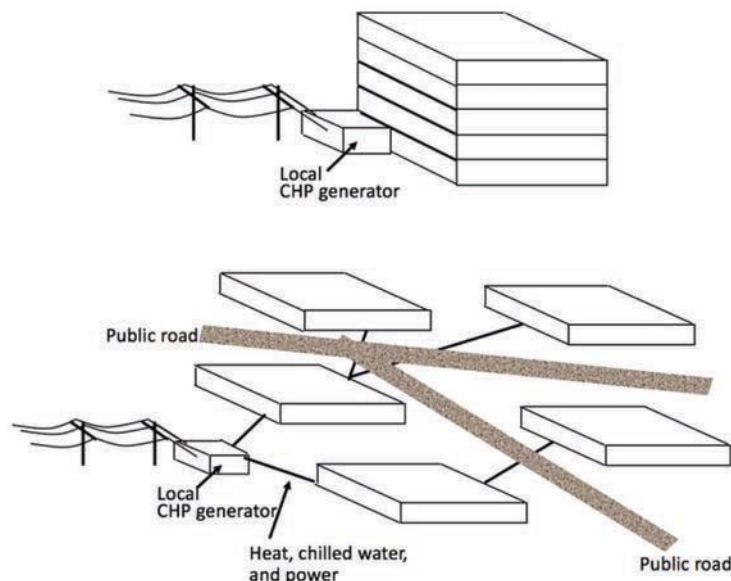
Closely linked to the way in which the future regulatory environment might evolve is the degree of penetration of distributed resources (Figure 2.11). The pace and extent of further deployment of DERs is the subject of major discussion in the industry. If the DOE SunShot targets are met, for example, rooftop solar will likely become cost competitive across much of the country without significant subsidies (Hagerman et al., 2016). Penetration of CHP has been much slower. Its future will depend in part on how the policy environment evolves and the wholesale-to-retail markup of natural gas. Costs are falling for local storage technology, but it is still only commercially viable in niche applications. Adoption could accelerate if costs fall and suppliers begin to offer storage with photovoltaic systems—with inverters and local intelligent control that reduces electricity bills and allows customers to continue to operate when grid power is unavailable.



**FIGURE 2.11** Different ways in which distributed resources might evolve in the future.

NOTE: CHP, combined heat and power; DER, distributed energy resource.





**FIGURE 2.12** Under most state laws, there is legal distinction between a utility that serves a multi-story building with its own distributed energy resource and combined heat and power, as shown at the top of this figure, and the situation in which the same loads are distributed across space and are served by a small microgrid. There is virtually no technical difference between these two situations. If laws were changed to allow private ownership of such microgrids (with equitable symmetric tariffs), future distribution systems could look very different. NOTE: CHP, combined heat and power.

There has been considerable discussion of smart controls for end-use devices, including the idea of “prices to devices” that would allow larger customers to decide when they will and will not operate particular electricity-using equipment given time-of-use pricing. While very extensive intelligent control is possible, what is less clear is when and whether the added hardware and intelligence will make economic sense.

### Legal Implementation of Non-Utility Microgrids

Today in most of the United States, state law grants exclusive service territories to legacy distribution utilities, although there are a few exceptions.<sup>25</sup> This means that with the exception of a customer selling power back to the local utility, only that utility can distribute power to another entity. It also means that only a traditional utility can move power across a public road or other public right-of-way. If state laws were changed in such a way as to allow small-scale microgrids (larger than a few MWs) to be operated by private

entities—with tariffs that symmetrically recognize the contributions of DERs while keeping the distribution company whole—the adoption of DERs could accelerate. Utility executives often argue that such a change would impose serious operational problems. However, from a technical point of view, there is very little difference between the two situations shown in Figure 2.12.

The committee asked several state regulatory agencies whether, in their jurisdictions, an entity other than the local distribution utility could build a small microgrid (e.g., less than a few 10s of MW), sell electric power to other entities, and be interconnected to the distribution utility. Several states noted that, as a matter of law, this was simply impossible in their states. Others indicated that the answer was more complex—an entity that wanted to engage in such activity would need to become a licensed and regulated utility. For example, staff of the Pennsylvania PUC said, “It is conceivable that an entity could perform such a function if they were properly licensed by the commission and the RTO and PJM. There may be some other legal factors that could limit their ability to sell power to entities other than the distribution utility and/or PJM Pennsylvania does allow net metering (see footnote 21) up to 3 MW.” Staff from the ICC noted, “Third parties that sell electric power to retail customers of an investor-owned utility must be licensed by the (ICC).” Staff of the New Hampshire Commission noted that in addition to having net metering, their state also has “group net metering (up to 1 MW).”

<sup>25</sup> New York is one exception where the state may grant multiple franchises to serve a particular location; however, it is then up to local municipalities to grant easements along public streets and roads in order for the utility to install necessary facilities. Some Pennsylvania communities have been granted multiple franchises resulting in different utilities’ distribution lines on opposite sides of the street with service drops to customers crossing overhead. Nonetheless, in most regions service franchises are granted exclusively to one provider.

For years, the regulatory framing under which electric power has been provided in the United States was built on a foundation of universal service—that is, that access to basic electric power is to some degree a right that all citizens should enjoy. Indeed, it was this belief that prompted the creation of the Rural Electrification Administration in 1935 to supply power across rural America to customers whose locations were too remote to be attractive to privately operated utilities.

Today, the technical capability exists to provide different levels of service to different customers. This raises policy questions about whether all customers deserve some basic level of reliable service on the grounds of equity. As discussed in Chapter 5 of this report, there are ways in which distribution systems that contain advanced automation and distributed generation could be “islanded” so as to provide some limited service in the event of a large-area, long-duration blackout of the bulk power system. How the incremental cost of such upgrades should be covered, and whether they should only be based on an end-use customer’s ability to pay, raises obvious issues of social equity.

Over time, there will likely be greater opportunities for customers to defect from the grid (i.e., provide all of their electricity needs with customer-owned generation and storage). The goal of ensuring that all customers have access to electricity service that is affordable and reliable, combined with society’s larger interest in assuring that a resilient electric system supports the availability of critical social services, suggests that policy makers should continue to pay close attention to this trend. Policy makers may need to pursue mechanisms that encourage grid integration as part of service and to ensure that grid defection does not adversely impact those customers who have no practical economic choice but to remain dependent on the electric system to serve their needs.

### Impacts of a Changing Climate

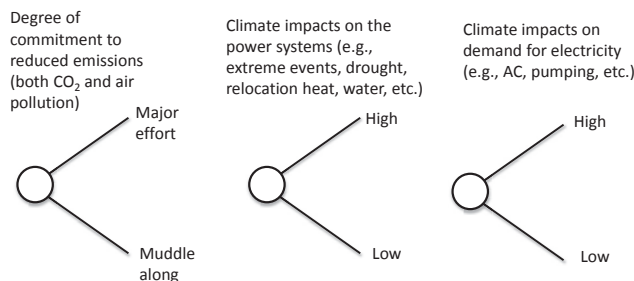
There remains uncertainty regarding how climate change and associated concerns will impact the electric power

system (Figure 2.13). While the impacts of climate change will unfold over the coming decades, policy choices made in the near future can have a profound impact on the extent of that change (White House, 2016). The changing climate will result in more frequent and more intense extreme events (Melillo et al., 2014) that will impose damage and other challenges on the power system. Higher ambient temperatures will create increased demand for system cooling. In some parts of the country, it will also bring deeper and more prolonged droughts that, in turn, will result in problems of securing sufficient water for system cooling unless traditional wet cooling is replaced with dry cooling. In some locations, such as coastal regions prone to rising sea levels and storm surge or inland locations prone to frequent wildfires or flooding, it may prove necessary to relocate some facilities. Climate change will likely also result in new demands for electric power including larger air conditioning loads and, in some locations, an increased demand for power to pump water.

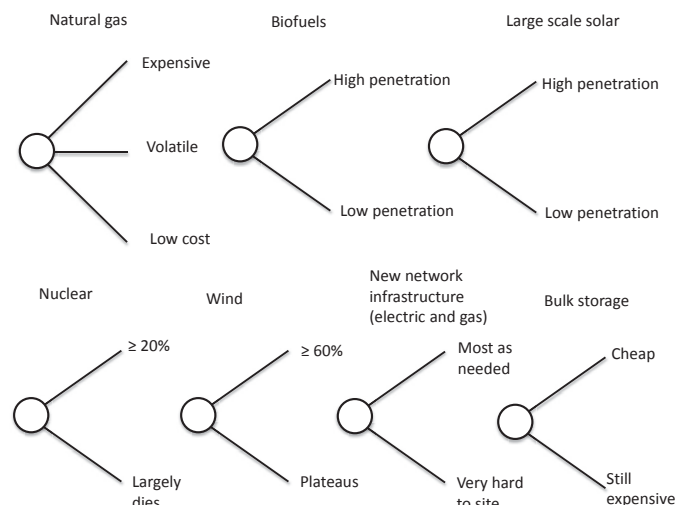
### Changes in the Sources of Bulk Power

The past few decades have seen dramatic shifts in the sources of bulk power employed in the United States, and uncertainty persists regarding the future (Figure 2.14). Natural gas has displaced generation at many coal-fired baseload power plants, and even existing nuclear plants are retiring before the end of their operating licenses. However, if prices once again become higher or more volatile, investors may shy away from putting capital into natural gas plants and the trend could be reversed, as it was in the past.

Many observers anticipate significant penetration of new renewables, especially wind, solar, and hydro power. Today, wind generation constitutes approximately 5 percent of total U.S. generation, but a number of analyses suggest that there is no technical reason why the nation could not generate more than 60 percent of its electricity from wind. However, achieving such a high level of penetration would impose considerable requirements on land use, both for siting the wind turbines and for constructing the necessary transmission infrastructure, much of which will need to cross state



**FIGURE 2.13** Climate change can affect, and be affected by, the power system.



**FIGURE 2.14** Possible change in the sources and nature of bulk power.

lines (MacDonald et al., 2016). Hence there is considerable uncertainty about the degree of future penetration of wind generation. Similar observations have been made with respect to solar generation. Many have argued that extensive use of biomass fuel, perhaps also with carbon capture and sequestration, will be necessary to achieve the objective of holding global warming to  $\leq 2^\circ\text{C}$ . At the same time, the widespread use of biomass imposes considerable logistical requirements and demands on land use (LaTourrette et al., 2011). Hence, it remains unclear how much future development will occur.

Nuclear power has contributed roughly 20 percent of the nation's electricity generation for the past few decades. Many forecasts of U.S. energy production continue to assume their continued contribution of roughly the same share of supply. With the cost pressures that nuclear plants are facing from inexpensive natural gas and subsidized renewables, and uncertainties about the cost and likelihood of life extension and relicensing, a number of plants have closed recently. New York state and Illinois recently adopted policies designed to keep existing plants operating (McGeehan, 2016). The only new plants under construction in the United States are in the service territory of vertically integrated utilities in the Southeast, where costs can be included in the rate base. In addition, the nation has largely abandoned aggressive research on more advanced reactor designs, so that for at least the next several decades the only options for new nuclear construction will likely be existing light-water reactor designs (DOE, 2017c; Ford et al., 2017). There may be some renewed interest in advanced reactor design research (DOE, 2017c), but the extent of programmatic support for this vision remains uncertain. Small modular reactors have received a lot of attention in part because they require less capital investment and offer much greater siting flexibility. Despite these benefits, however, long-standing efforts have

never reached commercial construction (Larson, 2016). Investment in new, small, and advanced reactors may require a number of changes in business models and reactor designs that allow standardized and quicker manufacturing of components and construction of reactors.

Today, technologies for cost-effective bulk storage are limited. Pumped hydro storage imposes considerable land use and other environmental costs, and only a few facilities for compressed air storage have been built. Battery storage is beginning to have some impact on the power system, especially in behind-the-meter applications. In 2012, DOE established the Joint Center for Energy Storage Research (JCESR) as one of its "Energy Innovation Hubs." JCESR's stated goal is to "deliver electrical energy storage with five times the energy density and one-fifth the cost" of present storage technologies (Crabtree, 2016). In addition to striving to develop batteries that would allow all electric passenger vehicles to be profitably marketed at a cost of approximately \$20,000 and with a range of 200 miles, JCESR director George Crabtree has articulated remarkably aggressive goals for affordable grid storage, including battery technology that would be competitive with pumped hydro storage, chemically based, and capable of seasonal storage. However, battery experts with whom the committee discussed the JCESR goals for bulk grid storage have expressed considerable doubt about achieving those goals, especially on the time scale of the next several decades.

Nonetheless, all electric vehicles with those capabilities would have an impact on both the transportation sector and on electricity demand. Whether or not the JCESR goals are met, a much higher penetration of electric or hybrid vehicles may well occur on the time scale of the next several decades. With greater adoption of electric and plug-in hybrid vehicles, there may be greater opportunities for using connected vehicle batteries to improve grid resilience—for example,

by using electric vehicle batteries to provide a fraction of a home's electricity demand during a large-area, long-duration outage (see Chapter 5).

## SUSTAINING AND IMPROVING THE RESILIENCE OF A GRID THAT IS CHANGING RAPIDLY AND IN UNCERTAIN WAYS

From all of the foregoing, five things are apparent:

1. The grid is undergoing dramatic change. This will be especially true over the next few years at the distribution level where DERs continue to increase and change the relationship of utilities to end users. While DERs may provide many opportunities to increase grid resilience, this will require regulatory changes and effective planning and coordination. Over the next decade or two, major changes are also likely in bulk power transmission.
2. Much of the hardware that makes up the grid is long lived, which limits the rate of change in the industry. However, over periods of a decade or two, many changes are possible, and it is virtually impossible to know how the future grid will evolve.
3. No single entity is in charge of planning the evolution of the grid. That will become ever more true as more and more players become involved, particularly regarding deployment and operation of DERs at the distribution level.
4. All players will be concerned about reliability, both for themselves and collectively. Only a few are likely to be focused in a serious way on identifying growing system-wide vulnerabilities or identifying changes needed to assure resilience.
5. Today, virtually no one has a primary mission of building and sustaining increased system-wide resilience or developing strategies to cover the cost of investments to increase resilience in the face of low probability events that could have very large economic and broader social consequences.

These five observations carry profound implications for the future resilience of the power system. In Chapter 3, the committee explores the many types of events that can give rise to large-area, long-duration outages. Chapters 4, 5, and 6 correspond to the three stages of the resilience framework illustrated in Figure 1.2, making specific recommendations in the course of the discussion. Finally, in Chapter 7 the committee both summarizes those recommendations and comes back to the broader implications of the five observations above to consider an integrated perspective to the issue of electricity system resilience and how best to assure that continued attention is directed at building and sustaining system-wide resilience of the nation's power system.

## REFERENCES

- ACEEE (American Council for an Energy-Efficient Economy). 2012. *Financial Incentives for Energy Efficiency Retrofits in Buildings*. Summer Study on Energy Efficiency in Buildings, Pacific Grove, Calif., August 12–17. <http://aceee.org/files/proceedings/2012/data/papers/0193-000422.pdf>.
- AEE (Advanced Energy Economy). 2015. "Can Utilities Get Smarter with Smart Meters." <http://blog.aee.net/can-utilities-get-smarter-with-smart-meters>. Accessed July 11, 2017.
- Alliance to Save Energy. 2013. *The History of Energy Efficiency*. Alliance Commission on National Energy Efficiency Policy, Washington, D.C., January. [https://www.ase.org/sites/ase.org/files/resources/Media%20browser/ee\\_commission\\_history\\_report\\_2-1-13.pdf](https://www.ase.org/sites/ase.org/files/resources/Media%20browser/ee_commission_history_report_2-1-13.pdf).
- APPA (American Public Power Association). 2014. *Evaluation of Data Submitted in APPA's 2013 Distribution System Reliability & Operations Survey*. [http://www.publicpower.org/files/PDFs/2013DSReliabilityAndOperationsReport\\_FINAL.pdf](http://www.publicpower.org/files/PDFs/2013DSReliabilityAndOperationsReport_FINAL.pdf).
- Bakke, G. 2016. *The Grid: The Fraying Wires Between Americans and Our Energy Future*. New York: Bloomsbury Press.
- Blumsack, S., L. Lave, and J. Apt. 2008. "Electricity Prices and Costs under Regulation and Restructuring." Paper presented at the 2008 Industry Studies Annual Conference, Boston, Mass., May 1–2. [http://web.mit.edu/is08/pdf/Blumsack\\_Lave\\_Apt%20Sloan%20paper.pdf](http://web.mit.edu/is08/pdf/Blumsack_Lave_Apt%20Sloan%20paper.pdf).
- BNEF (Bloomberg New Energy Finance). 2016. "Reactors in the Red: Financial Health of the U.S. Nuclear Fleet." <http://docplayer.net/26060517-Reactors-in-the-red-financial-health-of-the-us-nuclear-fleet.html>. Accessed June 28, 2017.
- BPA (Bonneville Power Administration). 2017. "Facts and figures." <https://www.bpa.gov/news/pubs/generalpublications/gi-bpa-facts.pdf>.
- CAISO (California Independent System Operator). 2017. "Western Energy Imbalance Market (EIM)." <https://www.caiso.com/informed/Pages/EIMOverview/Default.aspx>. Accessed July 13, 2017.
- CARB (California Air Resources Board). 2014. "Assembly Bill 32 Overview." <https://www.arb.ca.gov/cc/ab32/ab32.htm>. Accessed September 21, 2016.
- Crabtree, G. 2016. *Storage at the Threshold: Beyond Lithium-ion Batteries*. [http://renewableenergy.illinoisstate.edu/downloads/speaker-presentations/2016\\_energy\\_storage/2%20George%20Crabtree.pdf](http://renewableenergy.illinoisstate.edu/downloads/speaker-presentations/2016_energy_storage/2%20George%20Crabtree.pdf).
- De Martini, P., and L. Kristov. 2015. *Distribution Systems in a High Distributed Energy Resources Future*. Future Electric Utility Regulation Report No. 2, Lawrence Berkeley National Laboratory, October. [https://emp.lbl.gov/sites/all/files/FEUR\\_2%20distribution%20systems%2020151023.pdf](https://emp.lbl.gov/sites/all/files/FEUR_2%20distribution%20systems%2020151023.pdf).
- DOE (Department of Energy). 2015. "Modernizing the Electric Grid." *Quadrennial Energy Review First Installment: Transforming U.S. Energy Infrastructures in a Time of Rapid Change*. <http://energy.gov/epsa/downloads/quadrennial-energy-review-first-installment>. Accessed July 13, 2017.
- DOE. 2016a. "North American Electric Reliability Corporation Interconnections." [https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NERC\\_Interconnection\\_1A.pdf](https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NERC_Interconnection_1A.pdf).
- DOE. 2016b. "Residential Renewable Energy Tax Credit." <http://energy.gov/savings/residential-renewable-energy-tax-credit>. Accessed September 22, 2016.
- DOE. 2017a. *Quadrennial Energy Review: Transforming the Nation's Electricity System: The Second Installment of the QER*. January 2017. <https://energy.gov/epsa/downloads/quadrennial-energy-review-second-installment>. Accessed July 13, 2017.
- DOE. 2017b. *Modern Distribution Grid Vol. II: Advanced Technology Maturity Assessment*. [http://doe-dspx.org/wp-content/uploads/2017/03/Modern-Distribution-Grid\\_Volume-II\\_v1.1\\_03272017.pdf](http://doe-dspx.org/wp-content/uploads/2017/03/Modern-Distribution-Grid_Volume-II_v1.1_03272017.pdf).
- DOE. 2017c. *Vision and Strategy for the Development and Deployment of Advanced Reactors*. <https://energy.gov/sites/prod/files/2017/02/f34/71160%20VISION%20%20STRATEGY%202017%20FINAL.pdf>.



- DSIRE (Database of State Incentives for Renewables and Efficiency). 2016a. "Renewable Portfolio Standard Policies." <http://www.dsireusa.org/resources/detailed-summary-maps/>. Accessed July 13, 2017.
- DSIRE. 2016b. "3rd Party Solar PV Power Purchase Agreement (PPA)." <http://ncsolarcen-prod.s3.amazonaws.com/wp-content/uploads/2014/11/3rd-Party-PPA.pdf>.
- DSIRE. 2016c. "Net Metering." [http://ncsolarcen-prod.s3.amazonaws.com/wp-content/uploads/2016/07/Net\\_Metering1.pdf](http://ncsolarcen-prod.s3.amazonaws.com/wp-content/uploads/2016/07/Net_Metering1.pdf).
- DSIRE. 2016d. "Find Policies & Incentives by State." <http://www.dsireusa.org/>. Accessed September 22, 2016.
- EEI (Edison Electric Institute). 2017. "Industry Capital Expenditures." [http://www.eei.org/resourcesandmedia/industrydataanalysis/industryfinancialanalysis/QtrlyFinancialUpdates/Documents/EEI\\_Industry\\_Capex\\_Functional\\_2017.04.21.pptx](http://www.eei.org/resourcesandmedia/industrydataanalysis/industryfinancialanalysis/QtrlyFinancialUpdates/Documents/EEI_Industry_Capex_Functional_2017.04.21.pptx). Accessed July 13, 2017.
- EIA (Energy Information Administration). 2010. "Electricity: Status of Electricity Restructuring by State." [http://www.eia.gov/electricity/policies/restructuring/restructure\\_elect.html](http://www.eia.gov/electricity/policies/restructuring/restructure_elect.html). Accessed September 22, 2016.
- EIA. 2015. "What is U.S. Electricity by Generation Source?" <https://www.eia.gov/tools/faqs/faq.cfm?id=427&t=3>. Accessed September 22, 2016.
- EIA. 2016a. Electric Power Sales, Revenue, and Energy Efficiency. Form EIA-861, Detailed Data Files. <https://www.eia.gov/electricity/data/eia861/>. Accessed July 13, 2017.
- EIA. 2016b. *Monthly Energy Review*. <https://www.eia.gov/totalenergy/data/monthly/pdf/mer.pdf>.
- EIA. 2016c. "Preliminary Monthly Electric Generator Inventory." <http://www.eia.gov/electricity/data/eia860m/>. Accessed July 13, 2017.
- EIA. 2016d. "Today in Energy: Demand Trends, Prices, and Policies Drive Recent Electric Generation Capacity Additions." <http://www.eia.gov/todayinenergy/detail.cfm?id=25432>. Accessed September 20, 2016.
- EIA. 2016e. "Today in Energy: Solar, Natural Gas, Wind Make Up Most 2016 Generation Additions." <http://www.eia.gov/todayinenergy/detail.php?id=29212>. Accessed December 19, 2016.
- EPRI (Electric Power Research Institute). 2011. *Needed: A Grid Operating System to Facilitate Grid Transformation*. [https://www.smartgrid.gov/files/Needed\\_Grid\\_Operating\\_System\\_to\\_Facilitate\\_Grid\\_Transformati\\_201108.pdf](https://www.smartgrid.gov/files/Needed_Grid_Operating_System_to_Facilitate_Grid_Transformati_201108.pdf).
- EPRI. 2015. *The Integrated Grid: A Benefit-Cost Framework*. Final Report, 3002004878. Palo Alto, Calif.: EPRI.
- FERC (Federal Energy Regulatory Commission). 2016a. "Regional Transmission Organizations (RTO)/Independent System Operators (ISO)." <https://www.ferc.gov/industries/electric/indus-act/rto.asp>. Accessed July 13, 2017.
- FERC. 2016b. *Assessment of Demand Response and Advanced Metering*. <https://www.ferc.gov/legal/staff-reports/2016/DR-AM-Report2016.pdf>.
- Ford, M.J., A. Abdulla, M.G. Morgan, and D.G. Victor. 2017. Expert assessments of the state of U.S. advanced fission innovation. *Energy Policy* 108: 194–200.
- Glass, J. 2016. "Enhancing the Resiliency of the Nation's Electric Power Transmission and Distribution System," presentation to the Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System, September 29, Washington, D.C.
- GMLC (Grid Modernization Laboratory Consortium). 2017. *Grid Modernization: Metrics Analysis*. Richland, Wash.: Pacific Northwest National Laboratory.
- Gridwise Alliance. 2016. "3rd Annual Grid Modernization Index." [http://www.gridwise.org/report\\_download.asp?id=17](http://www.gridwise.org/report_download.asp?id=17). Accessed July 13, 2017.
- Hagerman, S., P. Jaramillo, and M.G. Morgan. 2016. Is rooftop solar PV at socket parity without subsidies? *Energy Policy* 89: 84–94.
- Hirschman, A. 1970. *Exit, Voice and Loyalty: Responses to Decline in Firms, Organizations and States*. Cambridge: Harvard University Press.
- Hoovers. 2017. "Arizona Public Service Company Revenue and Financial Data." [http://www.hoovers.com/company-information/cs/revenuefinancial.arizona\\_public\\_service\\_company.959a800ac6670f2a.html](http://www.hoovers.com/company-information/cs/revenuefinancial.arizona_public_service_company.959a800ac6670f2a.html). Accessed February 10, 2017.
- IEEE (Institute of Electrical and Electronics Engineers). 2013. *Standard for Interconnecting Distributed Resources with Electric Power Systems*. [http://grouper.ieee.org/groups/scc21/1547/1547\\_index.html](http://grouper.ieee.org/groups/scc21/1547/1547_index.html). Accessed July 13, 2017.
- IRC (ISO/RTO Council). 2015. "Members at a Glance." <http://www.isorto.org/About/Members/allmembers>. Accessed December 18, 2016.
- Karlin, B. 2012. *Public Acceptance of Smart Meters: Integrating Psychology and Practice*. ACEEE Summer Study on Energy Efficiency in Buildings. <http://aceee.org/files/proceedings/2012/data/papers/0193-000243.pdf>.
- Keogh, M., and C. Cody. 2013. *Resilience in Regulated Utilities*. National Association of Regulatory Utility Commissioners' Grants and Research Department, November. <https://pubs.naruc.org/pub/536F07E4-2354-D714-5153-7A80198A436D>. Accessed July 13, 2017.
- Kwasinski, A. 2016. Quantitative model and metrics of electric grids' resilience evaluated at a power distribution level. *Energies* 9(93).
- Larson, A. 2016. "Is There a Market for Small Modular Reactors?" *Power Magazine*, June 1. <http://www.powermag.com/market-small-modular-reactors/>. Accessed July 13, 2017.
- LaTourrette, T., D.S. Ortiz, I. Hlavka, N. Burger, and G. Cecchine. 2011. *Supplying Biomass to Power Plants: A Model of the Costs of Utilizing Agricultural Biomass in Cofired Power Plants*. Santa Monica, Calif.: Rand Corporation. [http://www.rand.org/content/dam/rand/pubs/technical\\_reports/2011/RAND\\_TR876.pdf](http://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR876.pdf).
- Lave, L.B., J. Apt, and S. Blumsack. 2004. Rethinking electricity deregulation. *The Electricity Journal* 17(8): 11–26.
- Lazard. 2015. *Lazard's Levelized Cost of Energy Analysis—Version 9.0*. <https://www.lazard.com/media/2390/lazards-levelized-cost-of-energy-analysis-90.pdf>.
- MacDonald, A.E., C.T. Clack, A. Alexander, A. Dunbar, J. Wilczak, and Y. Xie. 2016. Future cost-competitive electricity systems and their impact on US CO<sub>2</sub> emissions. *Nature Climate Change* 6: 526–531.
- McAnany, J. 2017. *2016 Demand Response Operations Market Activities Report*. <http://www.pjm.com/~media/markets-ops/dsr/2016-demand-response-activity-report.aspx>. Accessed July 13, 2017.
- McGeehan, P. 2016. "New York State Aiding Nuclear Plants with Millions in Subsidies" *New York Times*, August 1. [http://www.nytimes.com/2016/08/02/nyregion/new-york-state-aiding-nuclear-plants-with-millions-in-subsidies.html?\\_r=0](http://www.nytimes.com/2016/08/02/nyregion/new-york-state-aiding-nuclear-plants-with-millions-in-subsidies.html?_r=0). Accessed January 2, 2017.
- Melillo, J.M., T.C. Richmond, and G.W. Yohe. 2014. *Climate Change Impacts in the United States: The Third National Climate Assessment*. U.S. Global Change Research Program. doi:10.7930/J0Z31WJ2.
- MIT (Massachusetts Institute of Technology). 2011. *The Future of the Electric Grid*. <http://energy.mit.edu/wp-content/uploads/2011/12/MITEI-The-Future-of-the-Electric-Grid.pdf>.
- MIT. 2016. *Utility of the Future: An MIT Energy Initiative Response to an Industry in Transition*. <http://energy.mit.edu/wp-content/uploads/2016/12/Utility-of-the-Future-Full-Report.pdf>.
- NAE (National Academy of Engineering). 2003. "Greatest Engineering Achievements of the 20th Century." <http://www.greatachievements.org/>. Accessed September 22, 2016.
- NASEM (National Academies of Sciences, Engineering, and Medicine). 2016. *The Power of Change: Innovation for Development and Deployment of Increasingly Clean Electric Power Technologies*. Washington, D.C.: The National Academies Press.
- Navigant Research. 2013. *The Lithium Ion Battery Market*. [https://www.arpa-e.energy.gov/sites/default/files/documents/files/Jaffe\\_RANGE\\_Kickoff\\_2014.pdf](https://www.arpa-e.energy.gov/sites/default/files/documents/files/Jaffe_RANGE_Kickoff_2014.pdf).
- NERC (North American Electric Reliability Corporation). 2010. "Functional Model." <http://www.nerc.com/pa/Stand/Pages/FunctionalModel.aspx>. Accessed September 22, 2016.
- NERC. 2011. *Special Report: Spare Equipment Database System*. Atlanta: NERC.
- NERC. 2014. *NERC CIP-014 Physical Security Standards*. <http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-1.pdf>.
- NERC. 2016a. *Glossary of Terms Used in NERC Reliability Standards*. [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).

- NERC. 2016b. *Distributed Energy Resources: Connection, Modeling and Reliability Considerations*. <http://www.nerc.com/comm/Other/essntlrbltysrvckskfrDL/May%202016%20Meeting%20Materials.pdf>.
- NERC. 2017. "Critical Infrastructure Protection Compliance." <http://www.nerc.com/pa/CI/Comp/Pages/default.aspx>. Access March 13, 2017.
- NJBPU (New Jersey Board of Public Utilities). 2015. *Record of Decision*, May 21. <http://www.state.nj.us/bpu/pdf/boardorders/2014/20140521/5-21-14-2I.pdf>.
- NJBPU. 2017. In the Matter of the Petition of Rockland Electric Company for Approval of an Advanced Metering Program; and for Other Relief. BPU Docket No. ER16060524. [http://www.nj.gov/rpa/docs/ER16060524\\_Rate\\_Counsel\\_Initial\\_Brief\\_Rockland\\_AMI.pdf](http://www.nj.gov/rpa/docs/ER16060524_Rate_Counsel_Initial_Brief_Rockland_AMI.pdf). Accessed July 13, 2017.
- NRC (National Research Council). 2012. *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press.
- Parfomak, P.W. 2014. *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*. <https://fas.org/sgp/crs/homesecl/R43604.pdf>.
- PJM. 2016. *Load Forecast Report*, January. <http://www.pjm.com/~media/documents/reports/2016-load-report.ashx>. Accessed September 21, 2016.
- PJM. 2017. "Fact at a Glance." <https://www.pjm.com/~media/about-pjm/newsroom/fact-sheets/pjm-at-a-glance.ashx>. Accessed February 20, 2017.
- Platts. 2014. "Utility Service Territories of North America." <http://www.platts.com/products/utility-service-territories-north-america-map>. Accessed July 13, 2017.
- Plug-in America. 2016. "State and Federal Incentives." <https://pluginamerica.org/why-go-plug-in/state-federal-incentives/>. Accessed September 21, 2016.
- PNNL (Pacific Northwest National Laboratory). 2015. *The Emerging Interdependence of the Electric Power Grid & Information and Communication Technology*. PNNL-24643, August. [http://www.pnnl.gov/main/publications/external/technical\\_reports/PNNL-24643.pdf](http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24643.pdf).
- Reuters. 2010. "Smart Grid Skepticism Derails Baltimore Plan." <http://blogs.reuters.com/great-debate/2010/06/23/smart-grid-scepticism-derails-baltimore-plan/>. Accessed July 13, 2017.
- RGGI (Regional Greenhouse Gas Initiative). 2016. "CO<sub>2</sub> Auctions, Tracking & Offsets." <https://www.rggi.org/market>. Accessed September 21, 2016.
- SNL (Sandia National Laboratories). 2014. *Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States*. <https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/EnergyResilienceReportSAND2014-18019o.pdf>.
- SoCo (Southern Company). 2017. "Overview of Our Business." <http://www.southerncompany.com/about-us/our-business/home.cshtml#>. Accessed February 20, 2017.
- Spence, A., C. Demski, C. Butler, K. Parkhill, and N. Pidgeon. 2015. Public perceptions of demand-side management and a smarter energy future. *Nature Climate Change* 5: 550–554.
- State of New York. 2014. *Reforming the Energy Vision: NYS Department of Public Service Staff Report and Proposal*. CASE 14-M-0101. <http://www3.dps.ny.gov/W/PSCWeb.nsf/All/C12C0A18F55877E785257E6F005D533E?OpenDocument>. Accessed September 21, 2016.
- TCR (Tabors Caramanis Rudkevich). 2016. "Developing Competitive Electricity Markets and Pricing Structures." White paper prepared for New York State Energy Research and Development Authority and New York State Department of Public Service, Contract 64271. <https://www.hks.harvard.edu/hepg/Papers/2016/TCR.%20White%20Paper%20on%20Developing%20Competitive%20Electricity%20Markets%20and%20Pricing%20Structures.pdf>.
- Tierney, S. 2016a. *The U.S. Coal Industry: Challenging Transitions in the 21st Century*. <http://www.analysisgroup.com/uploadedfiles/content/insights/publishing/tierney%20-%20coal%20industry%20-%2021st%20century%20challenges%209-26-2016.pdf>.
- Tierney, S. 2016b. *The Value of "DER" to "D": The Role of Distributed Energy Resources in Supporting Local Electric Distribution System Reliability*. [http://www.cpuc.ca.gov/uploadedFiles/CPUC\\_PublicWebsite/Content/About\\_Us/Organization/Divisions/Policy\\_and\\_Planning/Thought\\_Leaders\\_Events/Tierney%20White%20Paper%20-%20Value%20of%20DER%20to%20D%20-%202016%20FINAL.pdf](http://www.cpuc.ca.gov/uploadedFiles/CPUC_PublicWebsite/Content/About_Us/Organization/Divisions/Policy_and_Planning/Thought_Leaders_Events/Tierney%20White%20Paper%20-%20Value%20of%20DER%20to%20D%20-%202016%20FINAL.pdf).
- USCB (U.S. Census Bureau). 2016. "QuickFacts." <http://www.census.gov/quickfacts/>. Accessed December 18, 2016.
- USDA (U.S. Department of Agriculture). 2016. "Rural Utilities Service." <https://www.rd.usda.gov/about-rd/agencies/rural-utilities-service>. Accessed July 13, 2017.
- White House. 2016. *Opportunities to Enhance the Nation's Resilience to Climate Change*. <https://www.whitehouse.gov/sites/default/files/finalresilienceopportunitiesreport.pdf>.
- Willis, H.H., and K. Loa. 2015. *Measuring the Resilience of Energy Distribution Systems*. Santa Monica, Calif.: RAND Corporation.



# 3

## The Many Causes of Grid Failure

### INTRODUCTION

A wide variety of events can cause disruption of the power system. As noted in Chapter 1, given the numerous and diverse potential sources of disruption, it is impressive that relatively few large-area, long-duration outages have occurred. The causes of outages differ in a number of important ways. Two of the most important differences are as follows: (1) how much warning system operators have that a disruption is coming so they can take protective action, and (2) how much of the physical and cyber control systems that make up the power system remain operative once the disruption has passed. Figure 3.1 categorizes disruptions by the amount of advance warning that operators and others are likely to receive and the amount of time it takes to recover. Figure 3.2 categorizes the range of damages that may result after a disruption occurs.

### DIFFERENT CAUSES REQUIRE DIFFERENT PREPARATION AND HAVE DIFFERENT CONSEQUENCES

Building a strategy to increase system resilience requires an understanding of a wide range of preparatory, preventative, and remedial actions and an awareness of how these actions impact planning, operation, and restoration over the entire life cycle of different kinds of grid failures. Strategies must be crafted with awareness and understanding of the temporal arc of a major outage, as well as how this differs from one type of event to another.

It is also important to differentiate between actions designed to make the grid more robust and resilient to failure (e.g., wind resistant steel or concrete poles rather than wood poles; opaque fences around substations to protect against damage from firearms) and those that improve the effectiveness of recovery (e.g., preemptive powering down of select pieces of the system to minimize damage). Some actions serve both strategies, some serve one but not the other, and some serve one while inhibiting the other. For example, good substation design with clear separation of functions makes

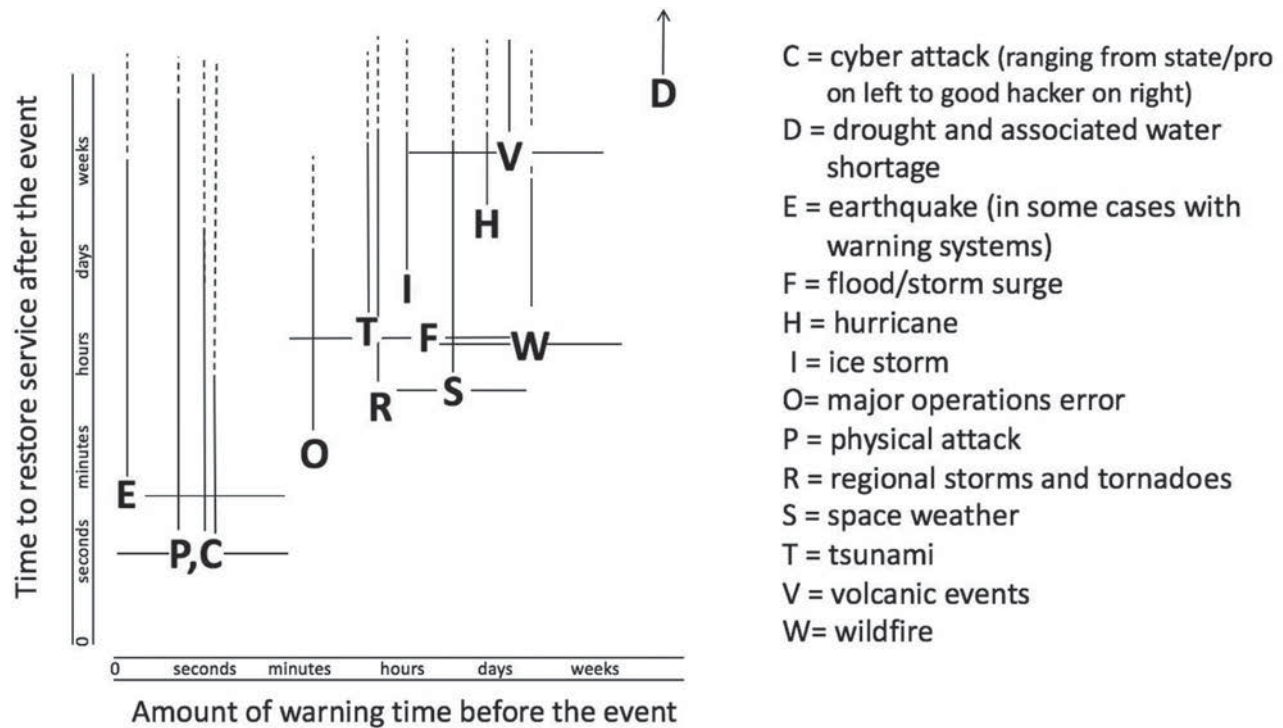
the substation more resistant to damage and helps repair crews. Building a coffer dam around a transformer may make it more resistant to flooding, but by limiting access for heavy equipment it can also make it harder to complete repairs when it actually fails. Of course a coffer dam does nothing to guard against the effects of earthquake or cyber attack. Similarly, concrete poles may be more resistant to wind but offer no clear advantage or disadvantage in restoration.

The timing of repairs is different depending on the cause. For example, repairs can begin immediately after a tornado has passed, but flooding following a hurricane can delay the start of repairs for weeks and impede restoration efforts. Good planning and preparation are essential to mitigating, ameliorating, and recovering from major outages effectively. Systems—both human and technical—must be built prior to grid failure to allow the responders to assess the extent of failure and damage, dispatch resources effectively, and draw on established component inventories, supply chains, crews, and communications. The next section reviews the major causes of outages depicted in Figure 3.1, beginning with those for which operators have the least warning and ending with those for which they have the most. The chapter then makes a number of general findings and recommendations related to both human and natural threats to the power system.

### REVIEWING THE CAUSES OF OUTAGES

#### Earthquake

Moving through Figure 3.1 from left to right, the first point is labeled E for earthquake. Especially in the West, the central Mississippi valley, the coastal area of South Carolina, and southern Alaska and Hawaii (Figure 3.3), the potential for disruption of major power system equipment by earthquake is significant. Severe damage to distribution poles, transmission towers, and substations can result. Generators may be damaged or subjected to enough stress that they have to be taken off-line. For example, the North Anna Nuclear Power Station was taken off-line following a magnitude 5.8



**FIGURE 3.1** Mapping of events that can cause disruption of power systems. The horizontal placement provides some indication of how much warning time there may be before the event. The vertical axis provides some indication of how long it may take to recover after the event. Lines provide a representation of variability in these estimates.

earthquake in Virginia in 2011 and remained off-line for more than 10 weeks as the owner and operator conducted thorough damage assessments and the Nuclear Regulatory Commission granted approval for restart (Vastag, 2011; Pelletier, 2012). In addition, there is substantial risk of the loss of fuel, particularly from natural gas systems, given the long supply chain and vulnerability of pipelines to earthquakes.

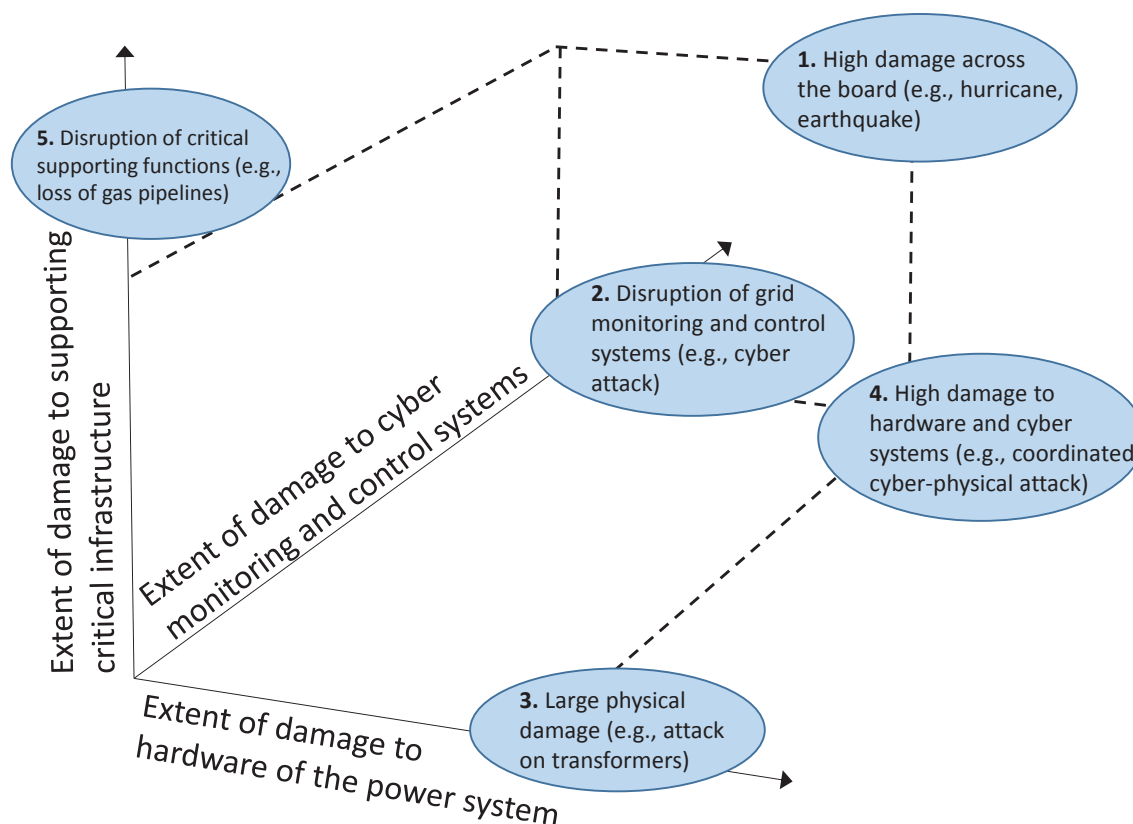
While earthquakes typically come without warning, the propagation velocity of earthquake waves is much slower than the speed of light, so that in some cases it is possible with appropriate instrumentation to obtain several seconds of advance warning (hence the horizontal line that runs to the right of point E in Figure 3.1). When possible, such warning could give time to de-energize critical components so as to minimize damage. Research is continuing on a wide range of grid-specific technologies. Organizations like the Pacific Earthquake Engineering Center are working on technologies such as more durable ceramic and non-ceramic insulators, flexible electrical connectors, and advanced materials for towers and attachments. Restoration following a major earthquake is a massive problem requiring a wide range of difficult engineering and construction projects in a compromised environment, with competition from other restoration priorities. For example, key bridges or roads required to access damaged facilities may be impassable. If an earthquake destroys key generating, substation, or transmission equipment, it may take weeks or months to restore service.

### Physical Attack

A physical attack, denoted by point P, could occur without warning or with only limited warning. Physical attacks on major system components could cause serious physical damage, especially to large transformers and other hard to replace substation and transmission equipment such as high-voltage circuit breakers. The possibility of such attacks has been a concern for many years (OTA, 1990; NRC, 2012; DOE, 2015; Parfomak, 2014). Globally, transmission and distribution systems have been a focus of physical attacks, bombings, and terrorist activity—for example, in Afghanistan, Colombia, Iraq, Peru, and Thailand (NRC, 2012). In the United States, there have been relatively few well-planned attacks on the electricity system, though the 2013 sniper attack of the Metcalf transmission substation (Box 3.1) provides a reminder of the physical vulnerability of the system. Recovery could easily require many days or weeks. Generation facilities tend to have greater physical security and thus are less vulnerable to physical attack than substation and transmission facilities.

### Cyber Attack

Like a physical attack, a cyber attack, denoted with a C, could also occur with limited or no warning. The best defense against cyber attacks is preventing intrusions to



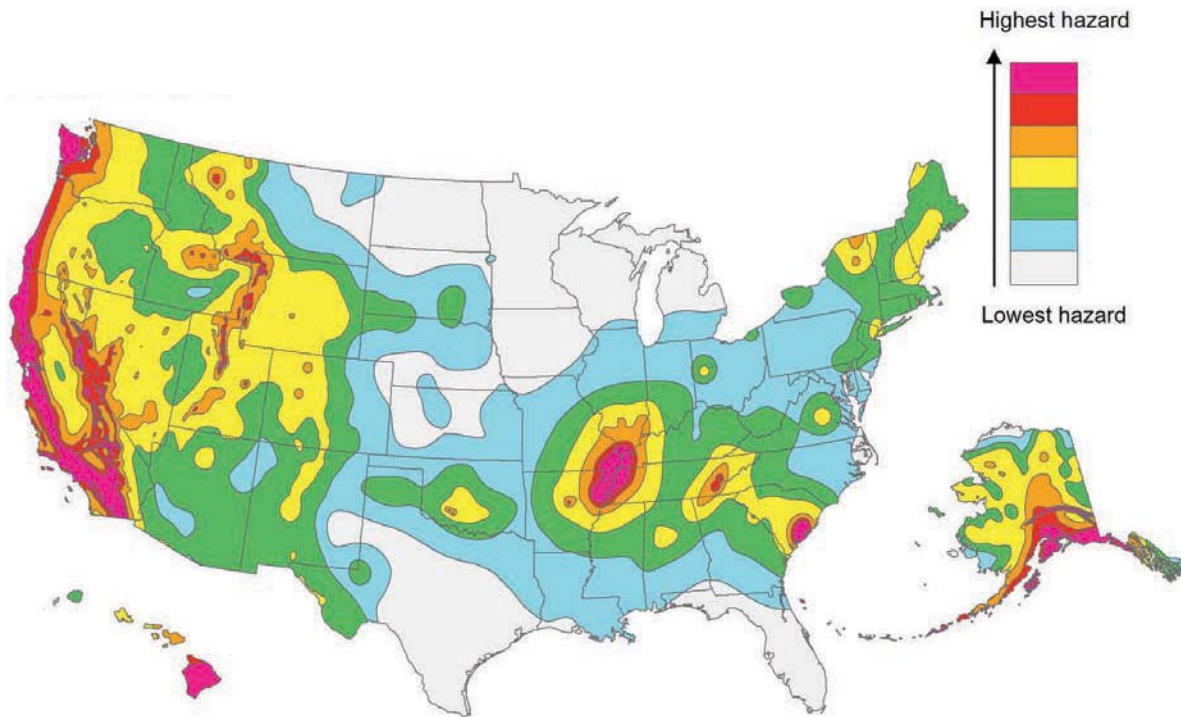
**FIGURE 3.2** Illustration of distinct types of damages that can affect power systems. Major disruptive events such as hurricanes or earthquakes can cause damage across the board—to the physical and cyber components of the power system and supporting critical infrastructure (case 1). While it is possible to do physical damage with a cyber attack, many cyber attacks would not give rise to physical damage but could cause considerable disruption in the ability to monitor and control the power system (case 2). In contrast, a terrorist attack on high-voltage transformers could result in extensive damage to critically important hardware while leaving monitoring and control capabilities intact (case 3). A coordinated cyber-physical attack can simultaneously cause serious physical damage to grid components and impede operators' ability to monitor and control the grid (case 4). Loss of other infrastructure such as natural gas pipelines or communication systems can have impacts on the ability of the system to operate (case 5).

critical systems and detecting and expunging malware before it becomes activated. However, if that is not possible, the consequences of a successful cyber attack may be almost instantaneous, they could take a few seconds to some minutes to be fully realized, or an attacker may lay dormant for months collecting information as happened in the 2015 cyber attack on the Ukrainian power system (Box 3.2). It is difficult to determine how many cyber attacks have been attempted against U.S. utilities, by what means, and with what consequences.

In the time between detection of an intrusion and manifestation of any consequences, it may be possible to take some steps to limit the potential disruptive impacts. In many cases a cyber attack may not give rise to major physical damage to the system, although in some circumstances physical damage can result, especially if the attackers are sophisticated. Depending on the nature of the attack, just how long it would take to restore is unclear. The unique issues associated with

cyber risks and restoration are discussed in Chapters 4 and 6. There are also diverse types of cyber attacks and vulnerabilities within the electricity system. According to recent analysis done for the Quadrennial Energy Review (Argonne National Laboratory et al., 2016), the electricity system vulnerabilities include the following:

- *Supervisory control and data acquisition systems* that rely on modern communication infrastructure to collect data and send control signals in both the bulk power system (generation and transmission) and at the substation level;
- *Large power plant distributed control systems* that use local communications channels to perform local control on large power plants;
- *Smart grid technologies*, including software-based components with communication capabilities, used to increase the reliability, security, and efficiency of



**FIGURE 3.3** U.S. Geological Survey assessment of earthquake hazard across the United States.  
SOURCE: Petersen et al. (2014).

the grid as well as communicate data between utilities and customers;

- *Distributed energy resources* that are connected to open networks for communication and can include smart inverters with remote access;
- *Supply chain* that might have vulnerabilities of legacy software systems from commercial vendors; and
- *Corporate communication networks* that might have an entry point to electricity systems' control networks.

The modern power system also makes extensive use of the global positioning system (GPS), especially for time synchronization. Hence, disruption of GPS by space weather, or through cyber attack, could cause disruption in the bulk power system.

### Operations Error

A number of historical blackouts have been caused by one or more faults, typically when the system is heavily loaded, that could have been managed if not for a sequence of subsequent operator errors. The network structure of the grid allows large-scale disruptions to result from distant, localized electrical faults, and system irregularities can propagate near instantaneously, generally through the work of protection relays acting unexpectedly to unusual system conditions. For example, the infamous 2003 Northeast

blackout was triggered by a simple fault—a tree caused a transmission line short circuit—but within hours it became the largest blackout in U.S. history, owing to two computer/software errors that caused a lack of situational awareness from grid operators. A smaller but similar cascading failure

### BOX 3.1 Summary of the Metcalf Substation Attack

In April 2013, the Pacific Gas and Electric-owned Metcalf Transmission Substation outside of San Jose, California, was attacked by one or more gunmen. The attack was well planned and executed, with the attacker(s) severing several fiber-optic cables to disrupt local communications prior to beginning the attack with military-style rifles. In the hour between when communications lines were cut and the first law enforcement officers arrived, 17 transformers had been seriously damaged as oil leaked from bullet holes allowing electric components to overheat. No major outages occurred, as operators were able to re-route power flows from nearby generators, but the attack caused more than \$15 million in damages. Of course, compared with the havoc that would result from a coordinated attack on multiple key substations, the Metcalf event was rather minor.



### BOX 3.2 Summary of the Cyber Attack on the Ukrainian Grid

In a recent, well-publicized cyber attack, approximately 225,000 people were left without power for approximately 6 hours on December 23, 2015, in Ukraine. The attackers gained access to internal networks of three utilities through spear-phishing<sup>a</sup> schemes, malware, and manipulation of long-known Microsoft Office macro vulnerabilities. Rather than try to engineer breaches through the firewall, the attackers patiently harvested the credentials needed to gain access to the supervisory control and data acquisition (SCADA) system and learned how to operate the SCADA software. The attackers executed a well thought out strategy, including the following:

- Creating virtual workstations inside SCADA systems that were trusted to issue system commands;
- Co-opting remote terminal units within SCADA systems to issue “open” commands to specific breakers at substations;
- Severing communications by targeting firmware in serial-to-Ethernet devices, making most unrecoverable;
- Installing and running a modified KillDisk program that deleted information on what was occurring while making recovery reboots nearly impossible;
- Shutting down uninterruptible power supplies at control centers; and
- Executing a large denial-of-service attack on utility call centers that prevented customers from reporting outages and reduced the utilities' understanding of the extent of outages.

These actions prevented operators from accessing the SCADA systems, left control centers without power, and left cyber monitoring and control systems inoperable. Service was restored by shutting off the SCADA system and resorting to manual operation. Although power was restored relatively quickly, control centers were not fully operational for months following the attack (E-ISAC and SANS ICS, 2016).

<sup>a</sup> Spear phishing is a targeted email that appears to be from a known business or individual but is not. It is designed to gain unauthorized access to internal systems by prompting the target to download unwanted software.

occurred in 2011 in the southwestern United States, when a problem at a single substation in Arizona grew into a major outage across Southern California in a few minutes.

There are a vast number of potential types of operations error—in both control rooms and in the field—that can lead to cascading blackouts, which makes planning difficult. Fortunately, because virtually all key components of the power system have protective devices that disconnect before damage can occur, cascading blackouts typically do not cause serious physical damage to system components beyond the initiating failure. Depending on system conditions and the nature of faults, operator error can unfold over periods of minutes to hours, and there may be opportunities to detect errors and take corrective action. With improved training and drilling, better instrumentation, improved situational awareness, and improved control methods, the risks of operator error leading to cascading failure have been, and can continue to be, reduced. At the same time, other external threats such as terrorist attacks and pandemics can place operators under stress and potentially increase the probability of errors. In Figure 3.1, operations errors are denoted by point O.

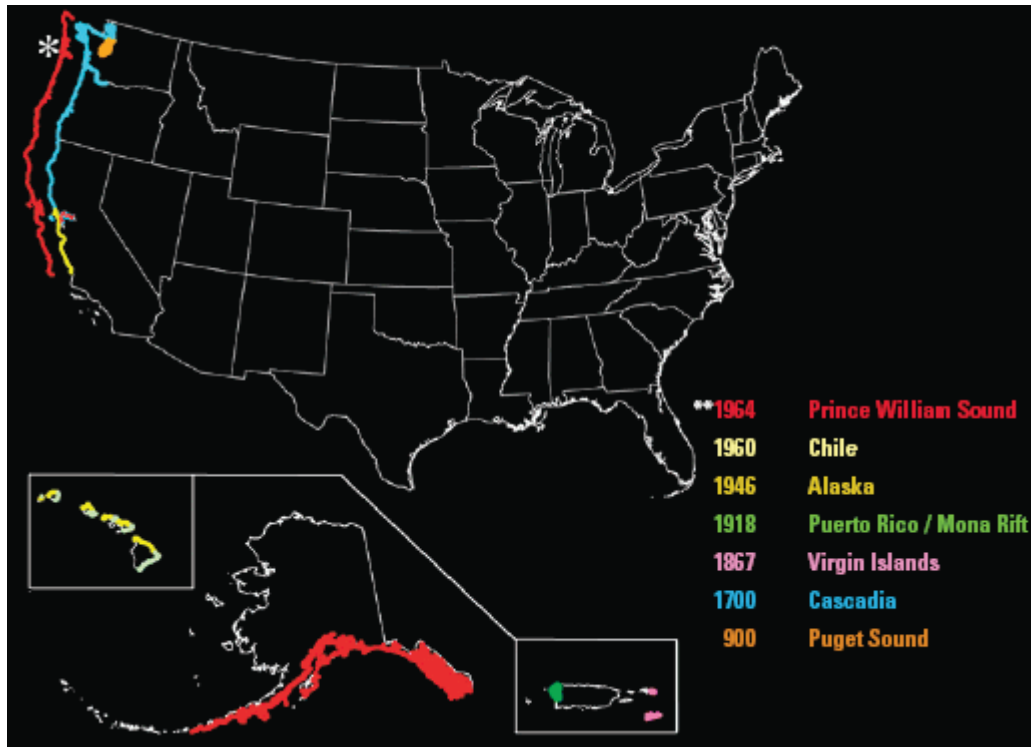
#### Tsunamis

The domain of damage for tsunamis, denoted T in Figure 3.1, is limited to coastal regions. Figure 3.4 shows

locations in the United States that have experienced major tsunami events over the past millennium, which are almost entirely on the Pacific coast. A large international warning system, involving 26 nations, monitors and provides warning across the Pacific basin. As part of that system, the United States hosts the Pacific Tsunami Warning Center near Honolulu, Hawaii, and also operates the Alaska Tsunami Warning Center in Palmer, Alaska. With advance warning, critical facilities can be shut down to reduce damage. Although the best way to reduce the risks to the power system is to place major facilities in locations that are not vulnerable to tsunamis, abandoning and moving existing installations is expensive, and there may be other protective steps that can be taken such as elevating backup generators. This is increasingly a factor in utility planning in Hawaii and along the West Coast.

#### Regional Weather

Weather events can be a major cause of disruption for the power system. Scientific knowledge about both the causes of severe weather events and the ability to detect changes in the risks varies considerably. Some changing risks, such as the likelihood of more frequent and extreme precipitation events and more frequent heat waves, are reasonably well understood in both regards. Others, like the frequency and

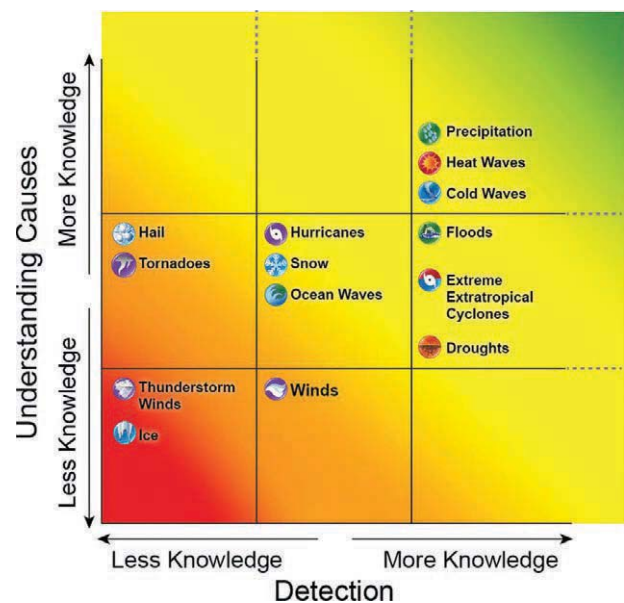


**FIGURE 3.4** U.S. coastal locations that have experienced major tsunamis over the course of the past 1,000 years.  
SOURCE: USGS (2016a).

intensity of ice storms (which can devastate power systems), are not understood in either regard. Figure 3.5 displays this considerable variation in the level of scientific understanding of weather and how the frequency and intensity of different weather events may evolve as a consequence of natural variability, climate system oscillations (El Niño–Southern Oscillation, North Atlantic Oscillation, etc.), and secular climate changes (IPCC, 2013; NASEM, 2016).

In Figure 3.1, point R denotes regional weather events such as intense convective storms and tornadoes that are capable of widespread damage, especially to distribution systems. Generally, individual tornadoes impact only a small area, and the specific locations at which damages occur are often difficult to anticipate. However, increasing resolution in weather forecasts does provide system operators with some ability to prepare and be ready to respond quickly once damage has occurred—for example, by pre-positioning repair crews.

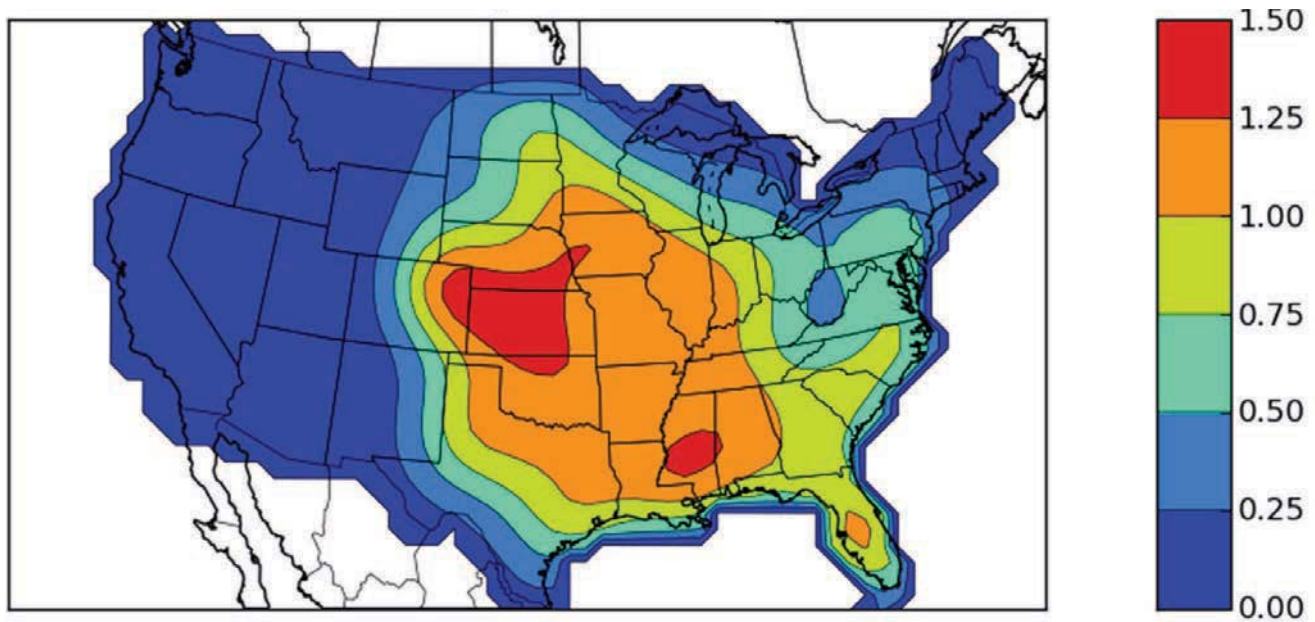
Tornadoes have occurred in all parts of the country, but they are rare west of the Rocky Mountains. Similarly, tornadoes do not occur at a uniform rate across the year and are most frequent in April, May, and June (Figure 3.6). Utilities and communities in high-frequency areas are aware of the risk and routinely prepare, building shelters for people and hardening the utility infrastructure.



**FIGURE 3.5** Summary of the state of knowledge of how the frequency and intensity of various weather events may evolve over time.

SOURCE: Wuebbles et al. (2014). ©American Meteorological Society. Used with permission.





**FIGURE 3.6** Map of tornado frequency from 1990 to 2009 (days per year within 25 miles of any point).  
SOURCE: NOAA and NSSL (2009).

The frequency of tornadoes shows a strong temporal and seasonal variation (Figure 3.7). The annual frequency of tornadoes strong enough to cause damage to power lines shows no apparent time trend. On the other hand, Tippet et al. (2016) report that “the largest U.S. effects of tornadoes results from tornado outbreaks . . . we find that the frequency of U.S. outbreaks with the many tornadoes is increasing and that it is increasing faster for more extreme outbreaks.” Tippet et al. (2016) report that, to date, they have been unable to link this increase to climate change. While not ruling out climate change, they speculate that low-frequency climate variability may be a contributing factor, among others. Figure 3.8 shows a track of storms on April 21 and 22, 2006, impacting four states from Mississippi to North Carolina. Often these different events are not connected by local authorities, each of which is responsible for recovery from a fraction of the total impact.

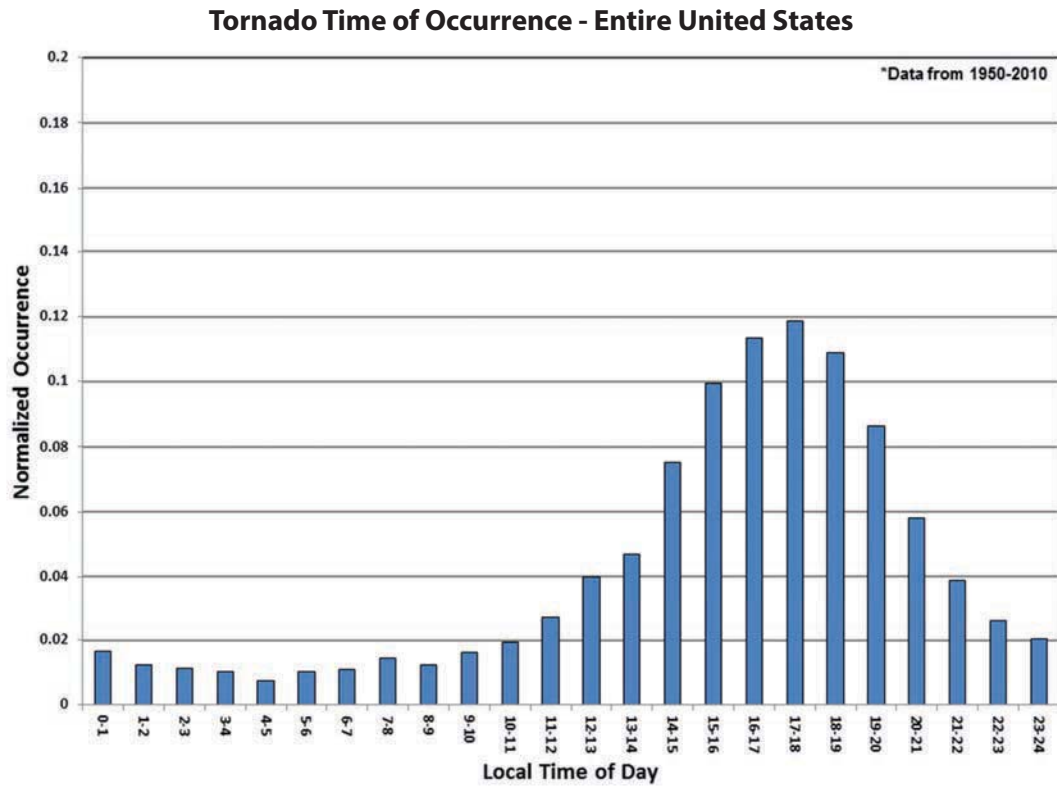
### Ice Storms

Point I in Figure 3.1 denotes ice storms (freezing rain). As is evident from the experience in 1998 in Québec, Ontario, and in upstate New York, ice storms (freezing rain) can result in very widespread damage after which full recovery may take many weeks. Figure 3.9A shows the historical distribution of freezing rain events in the United States over the past 50 years. Figure 3.9B shows the slight upward trend in event frequency over the period 1975 to 2014. Figure 3.9C shows the likely trend in the frequency of future ice storms across the different regions at risk. Ice storms interrupt power through the accumulation of ice on distribution and

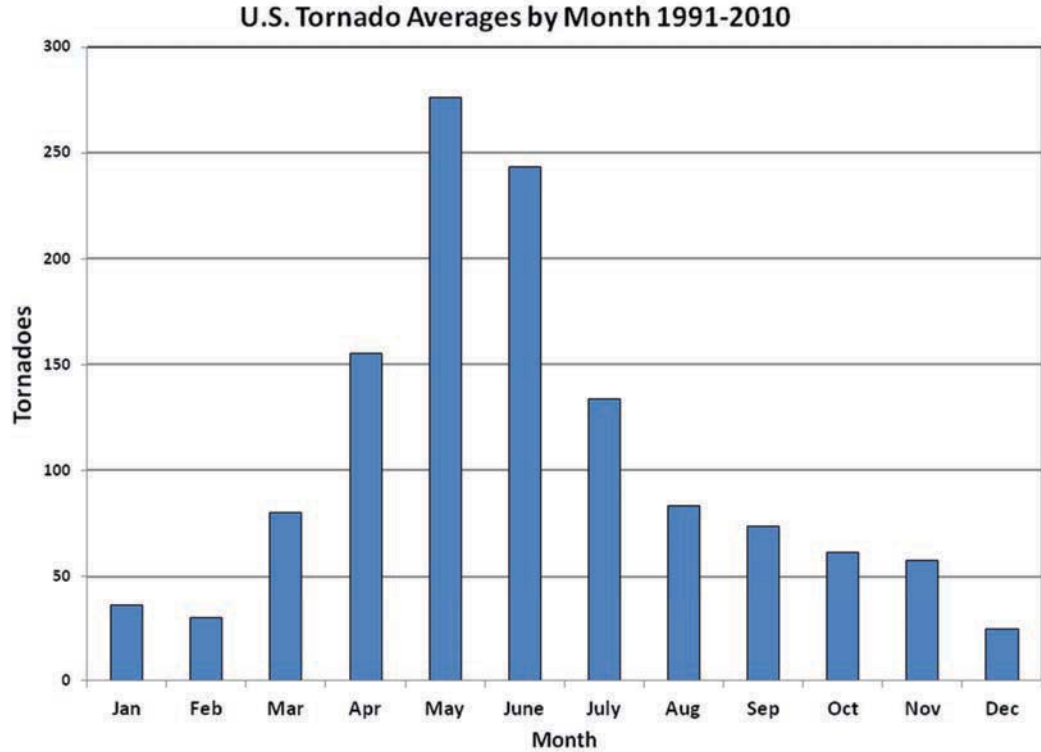
transmission lines, as the added weight brings lines down and causes damage to poles and towers. In addition to increased weight, wind blowing against ice-laden transmission lines can cause low-frequency (1 Hz) high-amplitude (1 m) oscillations (called conductor gallop) that further stress towers and insulators. Ice accumulation on nearby trees can cause branches to fall on lines or bring vegetation close enough to allow arcing current to cause a short. Impacts to distribution systems are common, whereas damage to transmission towers is less common but requires more resources and time to recover from. Many evocative pictures of damaged transmission and distribution infrastructure are available, dating back nearly 100 years. Figure 3.10A illustrates the extent to which ice can accumulate on distribution systems, and Figure 3.10B shows towers that collapsed due to ice accumulation during a massive storm in Québec in 1998. After the first tower failed, others were pulled down.

Winter storms are a leading cause of power outages nationally but do not receive as much national attention as concentrated events like hurricanes. However, they often do not meet Department of Energy (DOE) reporting requirements and might be exempt from the system average interruption duration index and the system average interruption frequency index reliability metric reporting. Because winter storm outages may be underreported, accurate statistics are not available. The majority of outages are relatively localized and handled by utility crews experienced with recovering from them. There are established and emerging techniques to reduce the risk of damage from ice storms and accelerate restoration. Building towers to higher standards is a known strategy, but there is insufficient data on the likelihood of

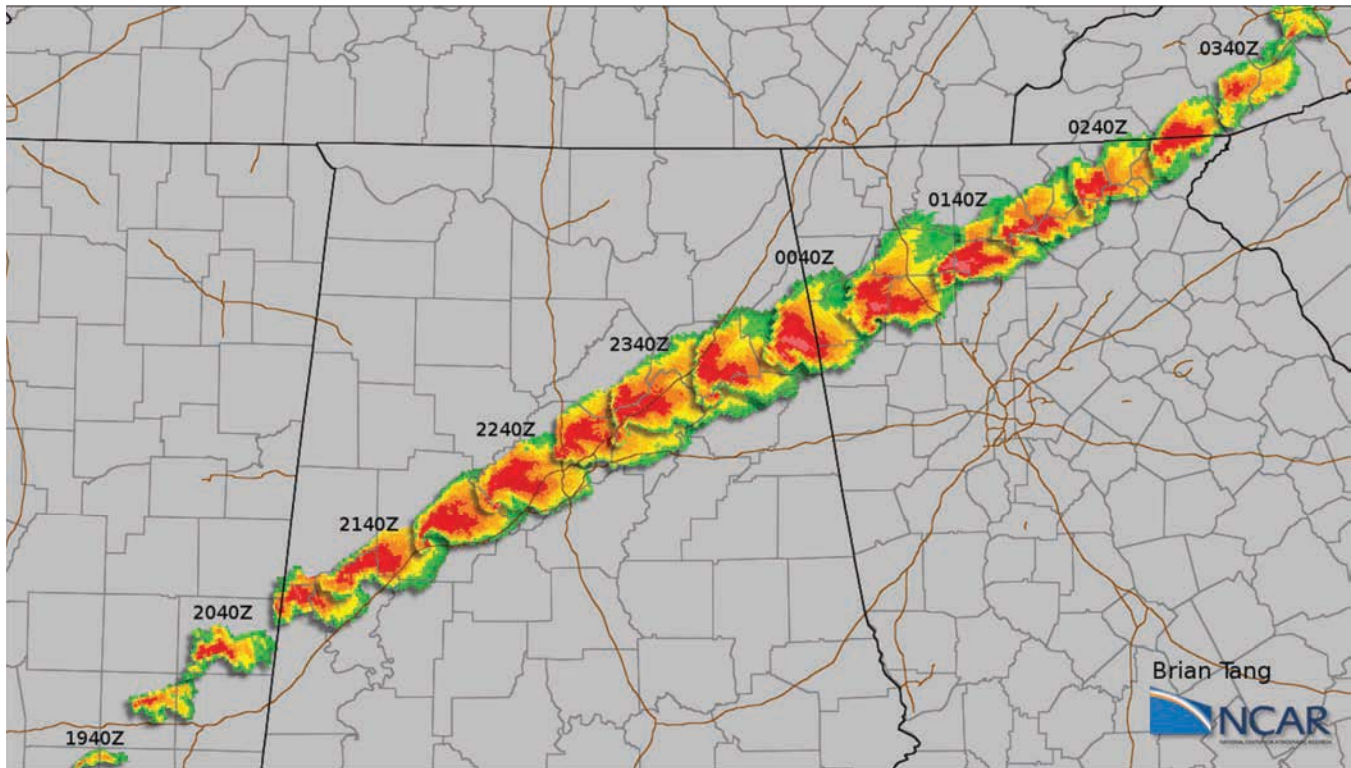
(A)



(B)



**FIGURE 3.7** Tornadoes show a strong (A) temporal and (B) seasonal variation.  
SOURCE: NOAA (2016).



**FIGURE 3.8** In 2006, a cluster of tornadoes caused damage across four states in 10 hours from one super cell.  
SOURCE: Tang (2008).

extreme ice events and the associated costs of outages to support greater investment. Techniques being explored for distribution systems include helically staked guying for poles, hydrophilic coating to help electrical infrastructure shed ice, and disconnecting wires that fall to the ground without damaging poles.

### Floods

Floods (Point F in Figure 3.1) can take many forms, from very abrupt flash floods that follow a sudden rainstorm or the breach of a dam, to events whose buildup occurs over extended periods. Floods can damage distribution or transmission towers and their footings or damage equipment installed on the ground. Most utilities have used historical flood data to choose locations for major facilities, such as substations, that are unlikely to be inundated. However, as the climate changes, the frequency of inundation is also changing (e.g., in some places a “100-year event” may have a much more frequent return period).

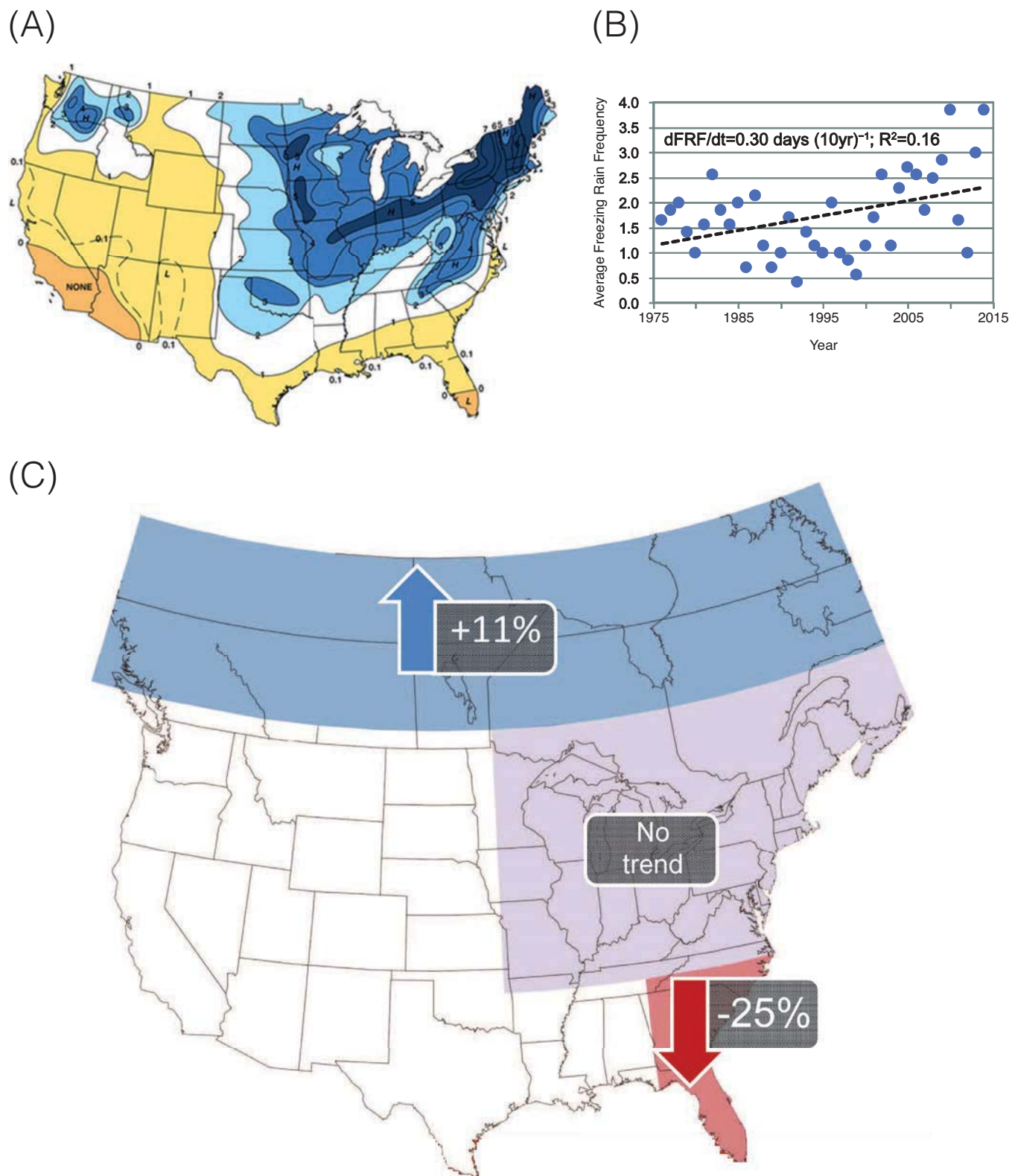
Hurricanes and tropical storms are a principal cause of flooding. Detailed maps of the “100-year flood plan” are available for much of the United States from the Federal Emergency Management Agency (FEMA). As of 2005, about one million miles of stream have been mapped. Figure 3.11 shows an example map for an area impacted by the flood following

Hurricane Agnes. The map reproduced here is compressed (and hence the legends are not readable), but it is included here to convey the type of information that is available.

The Intergovernmental Panel on Climate Change (IPCC) fifth assessment report anticipates that, in light of climate change, North America will experience “an increase in the number of heavy precipitation events” and “increased damages from river and coastal urban floods” (IPCC, 2014). These changes suggest that it is time to explore the development of more informative strategies to communicate the likely extent and frequency of future flooding since the traditional 30-year or 100-year flood metric is problematic when the underlying physical processes are not stationary.

The National Research Council Committee on Floodplain Mapping Technologies examined map accuracy in 2007 in a report titled *Elevation Data for Floodplain Mapping* and recommended much greater use of lidar altimetry (NRC, 2007). There are several challenges to accurate flood mapping, including these two: (1) the changes in the rate of river flows (and height of crest) as land is developed in a watershed, and (2) popular pressure to understate risk to lower flood insurance costs and avert an adverse impact on real estate value. Despite these limitations, the FEMA flood maps, if interpreted conservatively, provide a superb basis for assessing flood risks to electrical assets and planning flood remediation.



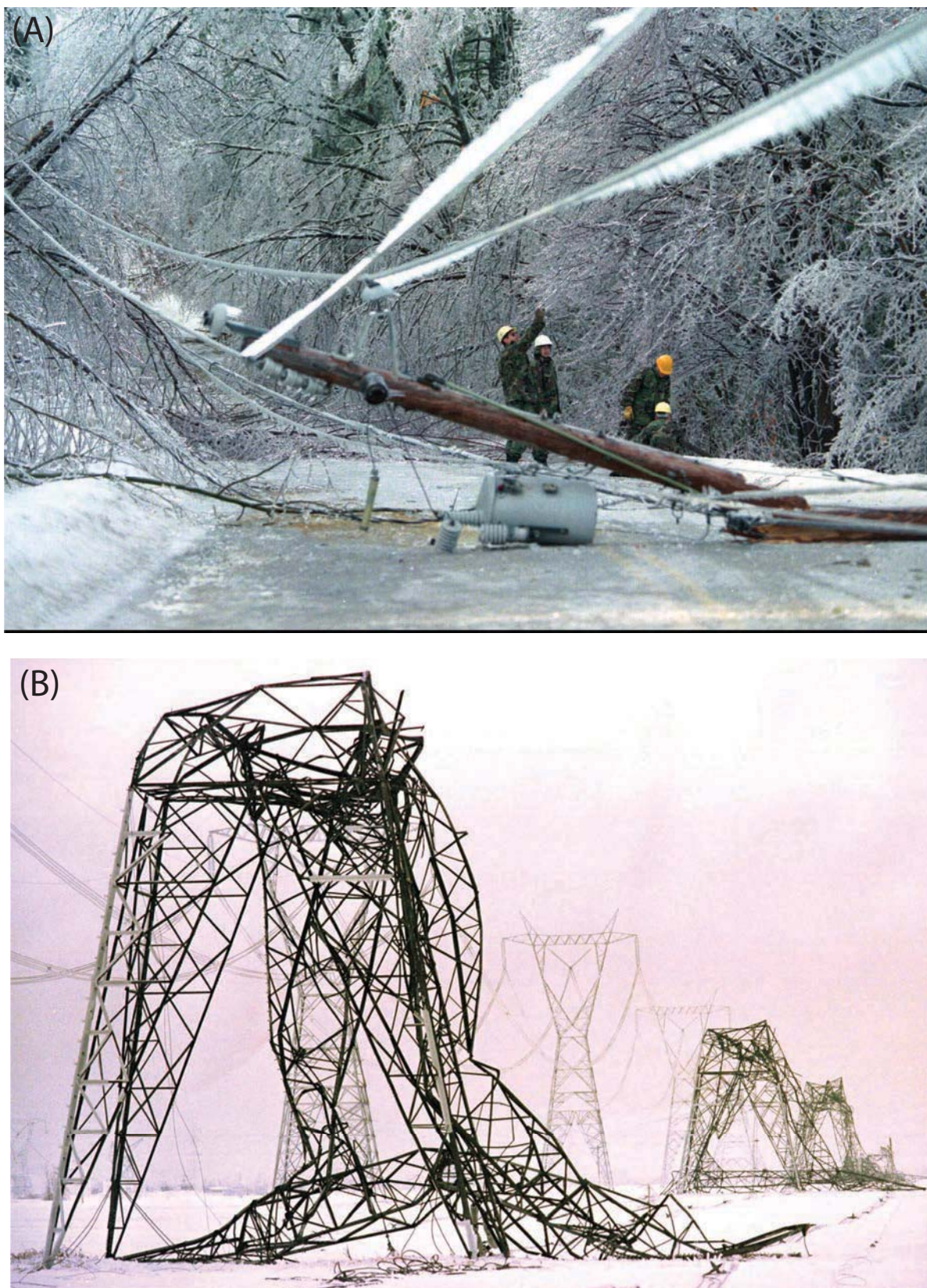


**FIGURE 3.9** (A) Distribution of freezing rain from 1948 to 2000, (B) slight recent trend toward more events, and (C) best estimate of trend by region.

NOTE: FRF, freezing rain frequency.

SOURCES: (A) Changnon and Karl (2003) ©American Meteorological Society. Used with permission. (B) Groisman et al./CC BY (2016). (C) Kunkel (2016).





**FIGURE 3.10** (A) Ice accumulation of several inches on distribution lines caused these poles to collapse, and (B) images from the infamous 1998 ice storm across southeastern Canada and the northeastern United States.  
SOURCE: (A) ©1998 The Associated Press (B) Robert Laberge/AFP/Getty Images.





**FIGURE 3.11** Example of a Federal Emergency Management Agency flood map for the Susquehanna River near West Pittston, Pennsylvania. The blue shaded areas on the east and west banks of the river are high risk. The dark gray areas beyond the blue area are at moderate risk. The areas outside of the shaded areas are not expected to be impacted by a 100-year flood. SOURCE: FEMA (2016).

In addition to disrupting the bulk power system, flooding can make access difficult for distribution system repair crews, cause damage by flooding manholes, and cause other problems in underground distribution systems and components. This suggests that care should be taken in design and building of underground systems in flood-prone areas.

### Space Weather and Other Electromagnetic Threats

A variety of solar activities (referred to as space weather, point S in Figure 3.1) can impact the earth's environment (NRC, 2008). Large bursts of charged particles ejected by storms on the sun, called coronal mass ejections, can intersect the earth, causing fluctuations in earth's magnetic field that create very low frequency voltage gradients across land, generally at northerly latitudes, and induce quasi-steady-state current that can flow in long transmission lines. These low-frequency currents can cause saturation of transformer magnetic cores and result in damage from overheating. Transformer saturation can also result in reactive power and harmonic generation, which can impact the entire power system. The largest storm of this type in the historical record is the 1859 Carrington Event, which caused telegraph systems

in the United States and Europe to fail. More recently, smaller solar storms have caused blackouts and very limited damage in power systems. In March 1989, approximately 6 million people lost power for up to 9 hours across Québec from a solar storm that damaged a few transformers and other equipment. A smaller hour-long outage occurred in Sweden in October 2003.

A risk summary prepared by Lloyds (2013) argues that “historical auroral records suggest a return period of 50 years for Québec-level storms and 150 years for very extreme storms, such as the Carrington Event.” In a 2011 study, the Department of Defense’s (DOD’s) JASON advisory panel concluded that the federal response to the risk “is poorly organized; no one is in charge, resulting in duplications and omissions between agencies” (MITRE, 2011). In 2015, the North American Electric Reliability Corporation (NERC) published a Notice of Proposed Rulemaking that requires transmission operators to conduct a vulnerability assessment and update it periodically (FERC, 2015). In October 2016, President Obama issued a comprehensive executive order addressing space weather, which gave the Department of Homeland Security overall leadership in geomagnetic disturbance preparedness and the DOE leadership in addressing grid impacts.

In 1989, there was no warning for the impending geomagnetic disturbance, whereas now satellites can provide 30 minutes of advance warning and sun observation up to 2–3 days ahead of impact. This warning could provide utilities an opportunity to protect the grid—for example, implementing operating procedures that are designed to protect critical transformers. The time constants determining impacts on transformers from solar storms (or from the E3 portion of electromagnetic pulse [EMP] events) are slow enough that there is time to protect transformers even as the event is occurring. Developing standard approaches for real time monitoring of transformers that could be susceptible to damage during solar storms (which can be identified through vulnerability assessments required by NERC) would help operators minimize damage. Such real-time monitoring could be combined with automated protection schemes that prevent transformer damage from geomagnetic disturbances. Other engineering solutions exist to make electrical systems more resistant to geomagnetic disturbances, including building better protection into transformers and designing systems to provide more reactive power on demand.

The National Oceanic and Atmospheric Administration (NOAA) and the U.S. Air Force jointly operate the Space Weather Prediction Center that uses solar and satellite observations (including NOAA’s DSCOVR satellite at the L1 point in deep space) to provide forecasts of space weather events. By observing the limb of the rotating sun, the addition of a satellite at L5 could provide valuable additional advance warning (Gibney, 2017). While coronal mass ejections are relatively slow moving, requiring a day or more to reach the earth, there are a number of events that can produce



highly energetic particles that can arrive at the earth in hours, sometimes with little or no warning. These high-energy particles can cause damage to GPS and other satellites, which are used by the power system.

Recent standards for transmission system performance in the event of geomagnetic disturbance (GMD)—for example, NERC standard TPL-007-1—are currently under revision but require that responsible entities maintain detailed system and geomagnetically induced current system models, use these to perform GMD vulnerability assessments every 5 years, and document and communicate this information to other affected entities.

Finally, the committee notes that several of the protective strategies that power companies adopt to reduce vulnerability to solar storms may also provide protection against the lower energy frequencies of an EMP,<sup>1</sup> which is a surge of electromagnetic radiation (Box 3.3) with different components that impact the power system. The early time component of an EMP (E1) is an intense, rapid pulse on the order of tens of kV per meter that decays to nearly zero in less than 1 microsecond; the intermediate time component (E2) has an amplitude of several hundred volts per meter and a duration of one to several hundred microseconds; and the late time component (E3) is a very low amplitude pulse on the order of millivolts per meter with a duration between 1 and 100 seconds. The electric fields associated with EMP can impact power systems directly (E1 and E2) or induce currents in transmission lines similar to the low frequency currents associated with GMD events (E3). Small, suitcase-size EMP devices<sup>2</sup> can also cause electromagnetic disturbances that can impact the power systems' (especially substation) equipment, but the impacts will likely be very localized. A nuclear weapon or a dedicated non-nuclear EMP device detonated at a high altitude could cause widespread damage to the electricity grid; nonetheless, understanding of this risk is largely theoretical. The Electric Power Research Institute (EPRI) collaborated with DOE recently to develop a Joint Electromagnetic Pulse Strategy that outlines broad objectives and research needs but stops short of presenting a plan for EMP hardening (DOE and EPRI, 2016).

While most critical satellites have been “hardened,” a large enough space weather event could cause damage to earth-orbiting satellites including those used for communication and the GPS. Modern utilities use the GPS to provide time synchronization across their spatially distributed systems. Disruption of these precise timing signals can result

<sup>1</sup> A continental-scale electromagnetic pulse caused by the detonation at high altitude of a specially designed nuclear weapon consists of several electromagnetic waveforms, the first of which has an extremely rapid rise time.

<sup>2</sup> “Suitcase-size EMP devices” are more accurately referred to as radio frequency weapons, essentially a class of non-nuclear weapons that have a local impact similar to that of an EMP E1 pulse. While the DOD is very experienced in this area, less attention has been directed to protecting civilian infrastructure. The concern is that one of these devices might target a control center, disrupting some or all of its computers and communications.

### BOX 3.3 Electromagnetic Pulse

An electromagnetic pulse (EMP) is a short duration surge of electromagnetic radiation that can be human-made or natural in origin and have local or widespread impacts. While local impacts can be caused by lightning strikes or by radio-frequency weapons, wider EMP impacts could be caused by the high-altitude detonation of an appropriately designed nuclear weapon. Such a wide-area EMP induced by a high-altitude nuclear weapon is an issue most appropriately addressed by the DOD.

The DOE and EPRI (2016) created the Joint Electromagnetic Pulse Resilience Strategy to help reduce the grid's vulnerability to EMP and improve the energy sector's response and recovery. The initial plan is more of a research strategy than an actual plan for EMP hardening and will take several years to realize. The plan sets five objectives:

1. Improve and share understanding of EMP threat, effects, and impacts;
2. Identify priority infrastructure;
3. Test and promote mitigation and protection approaches;
4. Enhance response and recovery capabilities to an EMP attack; and
5. Share best practices across government and industry, nationally and internationally.

in operational problems. While the GPS is well protected, it is also possible that sophisticated earth-bound hackers could disrupt GPS software and control systems. There are technologies that can minimize this risk, but to date their adoption has been limited (Achanta et al., 2015).

### Hurricanes or Tropical Cyclones

As we have learned repeatedly, tropical cyclones can create enormous havoc in power systems. Modern forecasting methods typically provide several days of advance warning, with increasingly more precise and accurate predictions about intensity and the location of landfall as a storm comes closer. Over their lifetime, tropical storms have three basic impacts on power systems: (1) initial impact of wind and rain, (2) storm surge in coastal areas and near major inland waters (e.g., Lake Pontchartrain during Katrina), and (3) flooding due to precipitation. Hurricane risk is concentrated on the Atlantic and Gulf coasts of the United States and in the state of Hawaii (Figure 3.12A).

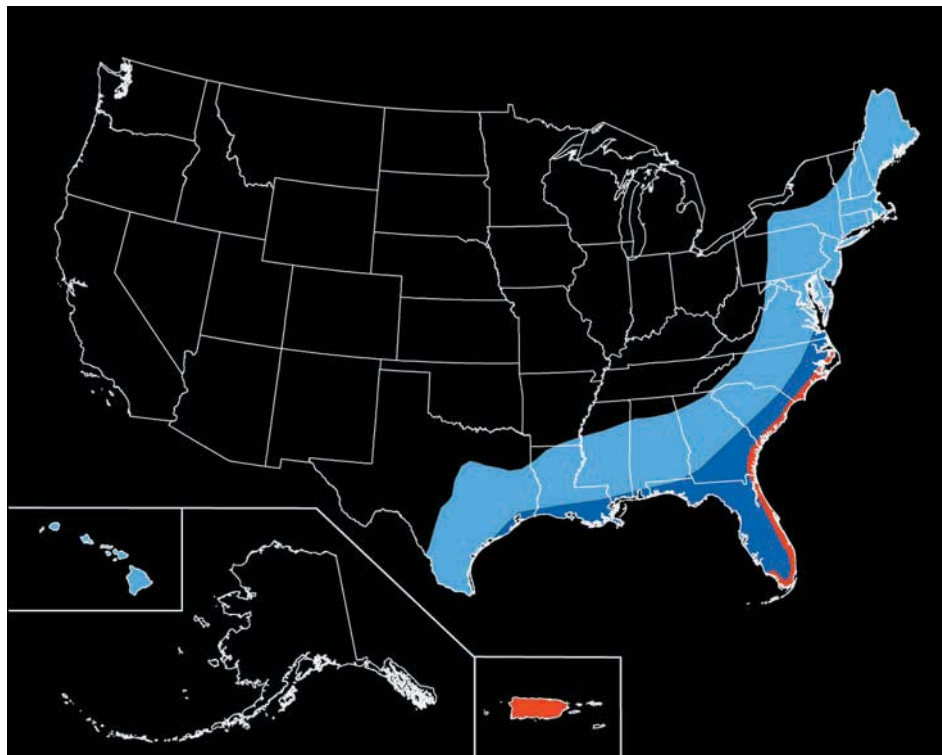
A 2016 report of the National Academies of Sciences, Engineering, and Medicine concludes that a “broad consensus

## THE MANY CAUSES OF GRID FAILURE

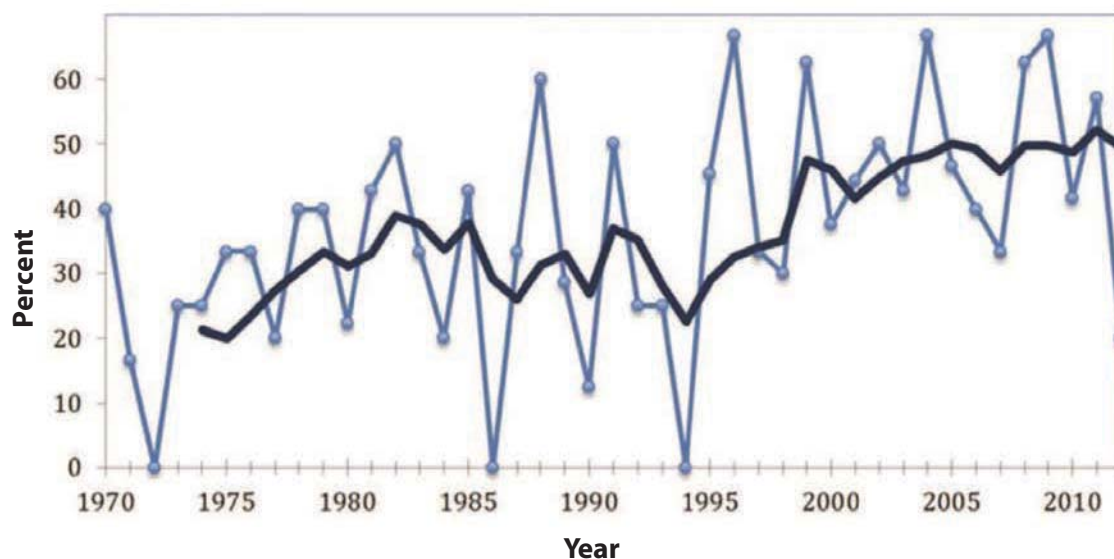
has emerged as to the expected future trends in their levels of certainty . . . tropical cyclones are projected to become more intense as the climate warms. There is considerable confidence in this conclusion . . . the global frequency of tropical

cyclone formation is projected to decrease . . . but there is less confidence in this conclusion than in the expectation of increasing intensity,” as indicated with historical data in Figure 3.12B (NASEM, 2016).

(A)



(B)



**FIGURE 3.12** (A) The region of hurricane risk is greatest on the Atlantic and Gulf coasts of the United States and (B) recent years have seen a trend of Atlantic hurricanes becoming more intense. This is probably the result of both warmer sea-surface temperatures and natural climate variations. The lighter color line is the percentage of hurricanes that reach category 3 or greater each year, and the dark is the 5-year running average.

SOURCE: (A) The National Atlas and USGS (2005) and (B) UCS (2016) at [www.ucsusa.org](http://www.ucsusa.org).

Along with winter storms, hurricanes and tropical storms<sup>3</sup> (Point H in Figure 3.1) are some of the largest sources of disruption of power systems. As illustrated by Superstorm Sandy and Hurricane Katrina, the resulting destruction can be widespread. Sandy was an immense and meteorologically complex storm that caused outages in 17 states and the District of Columbia, with the impacts beginning over a relatively short period of time. In contrast, Hurricane Katrina was a very different storm. While its impact on New Orleans (due largely to dike failures) and coastal Mississippi was the focus of press coverage, the total impact on electricity infrastructure was much broader because the storm had more rainfall, had higher sustained wind speed over larger areas, and traveled up the Mississippi River valley causing outages as far inland as Tennessee. Both Katrina and Sandy were devastating, but while Sandy was essentially a concentrated event, Katrina caused damage to power systems across a much larger region. While advanced models allow scientists to project the course and development of hurricanes with greater precision than ever before, weather events still have the capacity to surprise. In planning and preparation, it is important to remember that the evolution of a hurricane can involve substantial uncertainty.

### Volcanic Activity

In much of the country volcanic activity (V in Figure 3.1) is not a concern, but in the Pacific Northwest, and parts of Alaska and Hawaii, it presents a low probability but high consequence risk from eruption, ash fall, lava flow, and lahars. The U.S. Geological Survey maintains an active warning program (USGS, 2016b). Clearly the best strategy to avoid problems is to locate critical facilities away from vulnerable locations. However, as Figure 3.13 illustrates, in the case of Mount Rainier, the impacted region can be quite large. Additional damage can be caused by fine particulate dust and falling ash, which can cause insulator flashovers and potentially disable transformers. The geographic extent of falling ash may greatly exceed the immediate hazard area.

### Wildfire

Climate scientists have long predicted more frequent and more intense wildfires as a result of ongoing climate change (NCAR, 1988). While fire typically does not cause widespread damage to power systems, it can have major impacts on specific substations and transmission systems, and operators may have to re-route power flows to avoid affected areas. Vulnerability can often be limited with vegetation control, although very large fires can often jump even the most aggressive protective margins. Restoration of fire-damaged

facilities can require days or weeks. Fire is denoted as point W in Figure 3.1.

### Drought

Finally, in the extreme upper right corner of Figure 3.1 is point D, for drought. Droughts have multiple implications for power systems, ranging from reduced hydroelectricity generation, limited availability of cooling water for power stations, or increased demand for power needed for pumping and treatment. The IPCC report on extreme events concluded that “there is *medium confidence* that droughts will intensify in the 21st century in some seasons and areas, due to reduced precipitation and/or increased evapotranspiration. This applies to regions including . . . central North America” (Seneviratne et al., 2012).

While the power system can become very stressed during extreme heat (heat waves), ordinarily it manages to deal with such events. Of course, when the power system is highly stressed, the probability of hardware failures or operator error resulting in significant outages increases. The IPCC Fifth Assessment Report (2014, p. 10) concluded, “It is *virtually certain* that there will be more frequent hot and fewer cold temperature extremes over most land areas on daily and seasonal time scales, as global mean surface temperature increases. It is *very likely* that heat waves will occur with a higher frequency and longer duration.” The 2014 U.S. National Climate Assessment drew similar conclusions (USGCRP, 2014).

### Findings and Recommendations

The hazards reviewed in this section fall broadly into two categories: (1) those in which human action is the primary contributing factor, and (2) those that involve natural causes. The committee divides its findings and recommendations in this same way. With respect to hazards resulting from human actions, the committee finds the following:

**Finding:** While to date there have been only minor attacks on the power system in the United States, large-scale physical destruction of key parts of the power system by terrorists is a real danger. Some physical attacks could cause disruption in system operations that last for weeks or months.

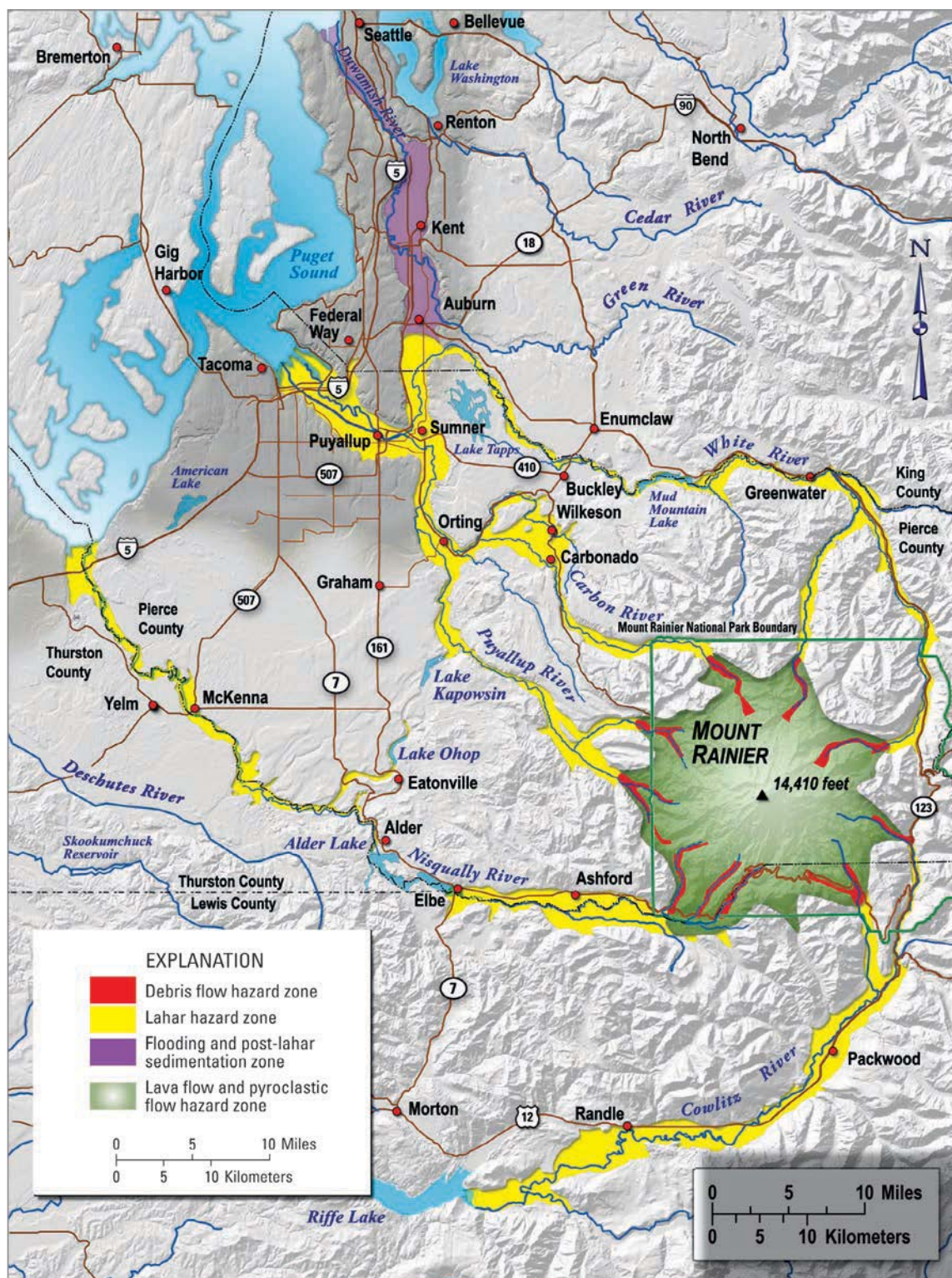
**Finding:** The United States has been fortunate that none of the cyber attacks that are being mounted against the power system have caused significant service disruption. However, the risks posed by cyber attacks are very real and could cause major disruptions in system operations.

**Finding:** While it is tempting to think of physical and cyber attacks as separate and discrete hazards, they could occur together and could also occur repeatedly. Furthermore, because the power system is essential to the operation of

<sup>3</sup> In this discussion, the committee includes post-tropical cyclones like Superstorm Sandy where most of the damage was done after the winds had dropped below hurricane force and the storm had lost its hurricane structure.



## THE MANY CAUSES OF GRID FAILURE



**FIGURE 3.13** Volcanic hazard map for the region around Mount Rainier. A “lahar” is a mud and debris flow that can bury everything in its path such as the communities marked as “hazard zones.”

SOURCE: USGS (2008).

many important infrastructures, physical and/or cyber attacks on that system can impact delivery of other critical services. An attack on the power system undertaken in conjunction with other terrorist action could be especially harmful.

**Recommendation 3.1:** To better protect the grid from physical and cyber attacks, the intelligence communities, the Department of Homeland Security, the Department of Energy, and operating utilities should sustain and enhance their monitoring and information-sharing activities and continue to assure that adequate communication channels are maintained among all responsible parties. Additional steps, such as the creation of teams to test weaknesses in existing systems, should be taken to avoid the risks of complacency and to drive a culture of continual improvement.

With respect to hazards resulting from natural causes, the committee finds the following:

**Finding:** Good data on the causes, probabilities, and spatial and temporal distribution of natural hazards that can disrupt power systems are essential to assuring the resilient operation of those systems. Government and other responsible parties should support and strengthen the activities of organizations that collect these data.

**Finding:** The probability, intensity, and spatial distribution of many of the hazards that can disrupt the power system are changing. These changes are due in part to the consequences of ongoing climate change. Traditional measures, based on an assumption of statistical stationarity (e.g., 100-year flood), may need to be revised to produce measures that reflect the changing nature of some hazards.

**Finding:** Some organizations that are responsible for monitoring and preparing for natural hazards, such as floods and tornadoes, have a local focus that can overlook spatial correlation and broader system risks. Nonetheless, local assessments such as the “Threat and Hazard Identification and Risk Assessment,”<sup>4</sup> encouraged by the Federal Emergency Management Agency, can provide valuable resources for utilities to build upon.

**Recommendation 3.2:** On a periodic basis (e.g., every 5 years), the Department of Homeland Security and the Department of Energy, as the energy sector lead, should work with state and local authorities and electricity system operators to undertake an “all-hazards” assessment of the natural hazards faced by power systems. Local utilities should customize those assessments to their local conditions and build on existing local assessments to include detailed electricity

system information, keeping in mind that the past may not be an accurate predictor of the future.

## THE LIFE CYCLE OF A POWER OUTAGE

Although the type and extent of damage varies among the different threats previously described, a notional time-series model of a power outage is shown in Figure 3.14, which provides elaboration of some of the key steps in the four-stage process of resilience displayed in Figure 1.2A. The committee also uses these steps in Chapter 6 to illustrate strategies to achieve resilience in the face of a specific cause of disruption.

The blue line in Figure 3.14 illustrates the percentage of load that may be served over time, from the initial full level until the start of the event, at which point load begins to drop off. Load persists at a reduced level for some period until restoration begins. Power is then restored, although sometimes not to the full pre-event level, as electricity-consuming entities may have been damaged or destroyed. If the event caused significant physical damage, load may continue to build slowly during a multi-year recovery period as electricity systems are restored, homes are reoccupied, and businesses reopen.

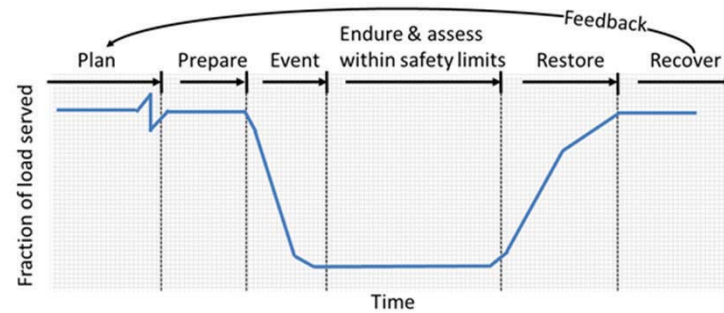
The relative length of each stage and the activities undertaken by utilities and other organizations involved in the response are different depending upon the type of disruption. Likewise, the activities undertaken by utilities during each of these stages also varies significantly based on the resources available and the technological characteristics of the impacted system. As briefly introduced below and as outlined in the following chapters, there are many strategies that can help utilities perform better through the entire outage life cycle.

## Plan

The majority of time is spent in the planning stage, which occurs continuously and well before any specific hazard is identified. While there is variation among organizations, utilities—from large vertically integrated firms to small distribution cooperatives—generally know what the major hazards are in their service territories, may have first-hand experience with such hazards, and may even be required by regulators to prepare and submit plans regularly for addressing these risks. For example, utilities in the Southeast prepare for hurricanes, whereas those in the far northeast focus more on ice storms. Utilities also generally know which parts of their physical systems are most vulnerable. This knowledge is acquired through experience and with diverse resources, such as data sets from NOAA and the National Weather Service. Nonetheless, the local impacts of most hazards, even those with a long history, are unknown during planning stages. Following Superstorm Sandy, the New Jersey utility Public Service Enterprise Group believed that the impact would have been much greater (perhaps double) if the storm track had been only 10 miles different, as more

<sup>4</sup> See, for example, [https://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201\\_htirag\\_2nd\\_edition.pdf](https://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf).





**FIGURE 3.14** Notional time series of a major power outage divided into six stages. The length of each stage and the activities performed by utilities and others involved in the response vary for different disruptions.

critical substations could have been affected by flooding in drainage basins. Utilities have less experience handling certain risks—notably those related to cyber attack—which makes assessing and planning more difficult.

Activities during the planning phase are both preventative and preparatory. At the distribution level, these include hardening system components and installing more advanced technologies such as automatically reconfigurable circuits. The level of investment by different utilities is closely tied to state regulatory or board oversight decisions; thus, there is wide variability across different states, and planning decisions are not solely determined by utilities. For investor-owned utilities, state regulatory commissions strive to keep costs low for ratepayers by approving investments that have net benefits for customers and not allowing a utility to “gold plate” its system. On the transmission level, utilities maintain, harden, and expand the physical and cyber infrastructure (both hardware and software) with investments and reliability standards overseen by NERC and FERC. As the complexity and scale of the grid as a cyber-physical system continues to grow, there are opportunities to plan and design the system to reduce the criticality of individual components and to fail gracefully as opposed to catastrophically. Equally important, utilities routinely plan for restoration—for example, by developing mutual assistance agreements, investing in spare parts sharing programs, and conducting restoration drills and exercises. Utilities must also engage and maintain strong relationships with local emergency management agencies to integrate their own planning into local and national efforts, as discussed in greater detail in Chapters 5 and 6. Additionally, there is a critical need to engage electricity end users during planning to define the locations and characteristics of critical loads in a service territory and ensure appropriate use of backup generation.

### Prepare

The preparation phase begins when a specific threat is identified—for example, when a hurricane forms with a projected track that will impact a specific utility. Some hazards have no advance warning, while others can be identified and

monitored with sufficient time for utilities and other responders to move beyond general planning and develop specific actions. For example, utilities preparing for impending hazard may check the health of critical components (including the health of cyber systems), check stocks of spare equipment, activate mutual assistance agreements, and bring local crews to a state of readiness, potentially pre-staging supplies and repair crews at specific locations. Operators assess the level of generation available, likely bringing additional reserve generation online, evaluate the adequacy and vulnerability of different fuel stocks and supply chains, and verify the state of charge of utility-scale storage assets if available. During preparation, utilities can begin coordinating with relevant disaster response organizations and encourage the public to purchase fuel and test backup generators. Utilities that have built and maintained strong relationships with local emergency management organizations know whom to engage, whereas organizations that have not built these relationships may waste valuable time and resources trying to connect with local efforts. There are growing opportunities to engage distributed energy resource (DER) owners so that system operators know the state of these resources, although current interconnection standards and contractual arrangements need to be revised to promote utility visibility and controllability of DERs.

### Event

The duration of disruptive events varies significantly, as do the capabilities and resources of different utilities. The duration of the actual disruptive event is always much shorter than the period from planning through final recovery. It can last many hours for hurricanes to minutes or even seconds for tornadoes and earthquakes. Floods can last many days or a small number of weeks. The longest duration, however, is for cyber events. The outage may only last a short time, but the period from cyber breach to detection and remediation may last many months. In the recent hack in Ukraine, the breach occurred 9 months before power was interrupted. The hackers used this time to learn how to control the breached systems.



Except in the case of a cyber attack, when the event may be ongoing for an extended period but undetected, the principal activity during the event is to monitor the damage and failures as they emerge and to develop as clear an understanding of system state as possible. Distribution systems with large amounts of advanced meter infrastructure and automated reconfiguration may lessen the number of customers experiencing outages. Some utilities may not be aware of outages until they are reported by telephone. Some events may be so destructive to physical and cyber systems that automation technologies have no benefit and could even be detrimental in the case of a cyber attack (e.g., if microprocessor-based relays with software installed by the manufacturer are hacked, the utility may have to replace the relay entirely or send it back to the manufacturer). There is a great deal of activity at the level of generation and transmission systems. System operators can balance generation and load through generation dispatch, load control (e.g., rolling blackouts), controllable DERs, or intentional islanding. It may be possible to continue with some preparatory activities, but, with limited time, telemetry, and communications, major changes may not be possible.

### Endure and Assess Within Safety Limits

For some events, conditions may prevent dispatch of crews (either boots on the ground or manned or unmanned aerial vehicles) because of safety concerns. This period may be zero (i.e., restoration can begin immediately), or it may stretch for a lengthy time if access to damaged facilities is blocked as by floodwater or landslides (utility crews can usually deal with downed trees). If cyber monitoring and control systems are intact, utilities can continue to assess the state of the system. During this phase, utilities communicate to understand the extent of damage, begin to prioritize repairs based on available information, and may even schedule the dispatch of restoration crews. As explained in Chapter 5 of this report, there are many strategies to reduce the adverse social and economic impacts of power outages, including using DERs, backup generators, and microgrids to provide local power to critical facilities.

### Restore

Restoration is the most tangible and publicly visible phase of the event life cycle. As soon as conditions permit safe dispatch of crews, utilities develop a high-resolution understanding of damages with manned and unmanned aerial vehicles as well as crews on the ground. Based on this understanding, priorities for restoration are established and repairs initiated, often through the shared resources previously arranged in mutual assistance agreements. If a critical transformer without a replacement is damaged, the system may have to be operated in a reduced state until a suitable replacement can be provided. System operators manage switching to

support physical restoration. Central operations also provide information to customers and support field crews by providing the necessary materials, replacement components, repair equipment, and qualified workers, as well as transportation and provisioning. This may require coordinating with state or federal officials to waive regulations or even using military resources in extreme cases. If there are regions of the interconnection with power, restoration may proceed from the “edge”; alternatively, utilities may initiate black-start<sup>5</sup> procedures. As installations of DERs continue to increase, there are growing opportunities to use these resources in restoration and black start; however, significant research is needed to demonstrate this capability.

### Recover

After the electrical grid has been repaired and service has been restored from a large-area, long-duration outage, utilities and regulators typically evaluate the event to identify root causes and opportunities to improve performance. These investigations directly inform planning and investment decisions made by utilities and overseen by regulators. As discussed in later chapters, there is often scrutiny of utility and infrastructure performance following a major outage, and there may be public and political support for grid investments that impact regulatory proceedings. In many cases (excluding cyber attacks and cascading failures) the commercial, residential, and public infrastructure are also damaged, may be long in returning, or may be lost permanently. In this case, the immediate restoration may be concluded, but the load served may be slightly or substantially less than prior to the event. Presuming the economy recovers and the impacted region is restored, the utility may be engaged in new construction for a number of years. At a minimum, this will entail a sustained period of increased capital spending and staffing for construction.

### REFERENCES

- Achanta, A., S.T. Watt, and E. Sagen. 2015. Mitigating GPS Vulnerabilities. Presented at the *Power and Energy Automation Conference*, Spokane, Wash. <https://selinc.com/api/download/104197/>. Accessed April 15, 2017.
- Argonne National Laboratory, Brookhaven National Laboratory, Los Alamos National Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories. 2016. *Resilience of the U.S. Electricity System: A Multi-Hazard Perspective*. <https://energy.gov/sites/prod/files/2017/01/f34/Resilience%20of%20the%20U.S.%20Electricity%20System%20A%20Multi-Hazard%20Perspective.pdf>.
- Changnon, S.A., and T.R. Karl. 2003. Temporal and spatial variations of freezing rain in the contiguous United States: 1948–2000. *Journal of Applied Meteorology* 42(9): 1302–1315.

<sup>5</sup> Most generators require power from the grid to energize their windings, which will not be available in the event of a major outage. “Black start” refers to the process of providing the necessary power to restore a generation plant when grid power is unavailable.

## THE MANY CAUSES OF GRID FAILURE

- DOE (Department of Energy). 2015. "Modernizing the Electric Grid." *Quadrennial Energy Review First Installment: Transforming U.S. Energy Infrastructures in a Time of Rapid Change*. <https://energy.gov/sites/prod/files/2015/08/f25/QUER%20Chapter%20III%20Electricity%20April%202015.pdf>.
- DOE and EPRI (Electric Power Research Institute). 2016. *Joint Electromagnetic Pulse Resilience Strategy*. [https://www.energy.gov/sites/prod/files/2016/07/f33/DOE\\_EMPStrategy\\_July2016\\_0.pdf](https://www.energy.gov/sites/prod/files/2016/07/f33/DOE_EMPStrategy_July2016_0.pdf).
- E-ISAC (Electricity Information Sharing and Analysis Center) and SANS ICS (Industrial Control Systems). 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. [https://ics.sans.org/media/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_5.pdf](https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf).
- FEMA (Federal Emergency Management Agency). 2016. "FEMA Flood Map Service Center." <http://msc.fema.gov/portal>. Accessed February 28, 2017.
- FERC (Federal Energy Regulatory Commission). 2015. "FERC Proposes New Reliability Standard on Geomagnetic Disturbances." <https://www.ferc.gov/media/news-releases/2015/2015-2/05-14-15-E-1.asp#.WJS-5jm8rLGh>. Accessed March 2017.
- Gibney, E. 2017. Europe lines up for solar storm view. *Nature* 541: 271.
- Groisman, P.Y., O.N. Bulygina, Y. Xungang, R.S. Vose, S.K. Gulev, I. Hanssen-Bauer, and E. Førland. 2016. Recent changes in the frequency of freezing precipitation in North America and Northern Eurasia. *Environmental Research Letters* 11(4): 045007.
- IPCC (Intergovernmental Panel on Climate Change). 2013. *Climate Change 2013: The Physical Science Basis*. Contribution of Working Group I to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change (T.F. Stocker, D. Qin, G.-K. Plattner, M. Tignor, S.K. Allen, J. Boschung, et al., eds.). Cambridge: Cambridge University Press.
- IPCC. 2014. *Climate Change 2014: Synthesis Report*. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change (Core Writing Team, R.K. Pachauri, and L.A. Meyer, eds.). IPCC, Geneva, Switzerland. [http://ar5-syr.ipcc.ch/ipcc/ipcc/resources/pdf/IPCC\\_SynthesisReport.pdf](http://ar5-syr.ipcc.ch/ipcc/ipcc/resources/pdf/IPCC_SynthesisReport.pdf).
- Kunkel, K. 2016. "NOAA Cooperative Institute for Climate and Satellites (NC State)." Presentation to the Committee on Enhancing the Resilience of Nation's Electric Power Transmission and Distribution System on July 11. Washington, D.C.
- Lloyds. 2013. *Solar Storm Risk to the North American Electric Grid*. <https://www.lloyds.com/~media/lloyds/reports/emerging%20risk%20reports/solar%20storm%20risk%20to%20the%20north%20american%20electric%20grid.pdf>.
- MITRE. 2011. *Impacts of Severe Space Weather on the Electric Grid*. <https://fas.org/irp/agency/dod/jason/spaceweather.pdf>.
- NASEM (National Academies of Sciences, Engineering, and Medicine). 2016. *Attribution of Extreme Weather Events in the Context of Climate Change*. Washington, D.C.: The National Academies Press.
- National Atlas and USGS. 2005. "Hurricane Hazards—A National Threat." [https://walrus.wr.usgs.gov/infobank/programs/html/factsheets/pdfs/2005\\_3121.pdf](https://walrus.wr.usgs.gov/infobank/programs/html/factsheets/pdfs/2005_3121.pdf). Accessed July 13, 2017.
- NCAR (The National Center for Atmospheric Research). 1988. "NCAR Co-Hosts Wildfire Severity and Global Climate Change Workshop." <https://opensky.ucar.edu/islandora/object/archives%3A883>. Accessed July 13, 2017.
- NOAA (National Oceanic and Atmospheric Administration). 2016. "Historical Records and Trends." <https://www.ncdc.noaa.gov/climate-information/extreme-events/us-tornado-climatology/trends>. Accessed February 28, 2017.
- NOAA and NSSL (National Severe Storms Laboratory). 2009. "Tornado Days (1990–2009)." Oklahoma Climatological Survey. [http://climate.ok.gov/index.php/climate/map/tornado\\_days\\_1990\\_2009/tornadoes\\_severe\\_storms](http://climate.ok.gov/index.php/climate/map/tornado_days_1990_2009/tornadoes_severe_storms). Accessed February 28, 2017.
- NRC (National Research Council). 2007. *Elevation Data for Floodplain Mapping*. Washington, D.C.: The National Academies Press.
- NRC. 2008. *Severe Space Weather Events—Understanding Societal and Economic Impacts: A workshop report*. Washington, D.C.: The National Academies Press.
- NRC. 2012. *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press.
- OTA (Office of Technology Assessment). 1990. *Physical Vulnerability of Electric System to Natural Disasters and Sabotage, OTA-E-453*. Washington, D.C.: U.S. Government Printing Office.
- Parfomak, P. 2014. *Physical Security of the U.S. Power Grid: High-Voltage Transformers Substations*. <https://fas.org/spp/crs/homesec/R43604.pdf>.
- Peltier, R. 2012. "Dominion's North Anna Station Sets New Standard for Earthquake Response." *Power*, November 1. <http://www.powermag.com/dominions-north-anna-station-sets-new-standard-for-earthquake-response/?pagenum=3>. Accessed April 28, 2017.
- Petersen, M.D., M.P. Moschetti, P.M. Powers, C.S. Mueller, K.M. Haller, A.D. Frankel, Y. Zeng, et al. 2014. *Documentation for the 2014 Update of the United States National Seismic Hazard Maps*. U.S. Geological Survey, Open-File Report 2014–1091.
- Seneviratne, S.I., N. Nicholls, D. Easterling, C.M. Goodess, S. Kanae, J. Kossin, Y. Luo, et al. 2012. Changes in climate extremes and their impacts on the natural physical environment. Pp. 109–230 in *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation* (C.B. Field, V. Barros, T.F. Stocker, D. Qin, D.J. Dokken, K.L. Ebi, M.D. Mastrandrea, et al., eds.). A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change (IPCC). Cambridge: Cambridge University Press.
- Tang, B. 2008. "National Center for Atmospheric Research." <http://www.ustornadoes.com/wp-content/uploads/2014/04/brian-tang-april27-ncar.png>. Accessed July 13, 2017.
- Tippett, M.K., C. Lepore, and J.E. Cohen. 2016. More tornadoes in the most extreme U.S. tornado outbreaks. *Science* 354(6318): 1419–1423.
- UCS (Union of Concerned Scientists). 2016. "Hurricanes and Climate Change." [http://www.ucsusa.org/global\\_warming/science\\_and\\_impacts/impacts/hurricanes-and-climate-change.html#.WJS9OW8rLGg](http://www.ucsusa.org/global_warming/science_and_impacts/impacts/hurricanes-and-climate-change.html#.WJS9OW8rLGg). Accessed November 27, 2016.
- USGCRP (U.S. Global Change Research Program). 2014. "National Climate Assessment." <http://nca2014.globalchange.gov/>. Accessed July 13, 2017.
- USGS (U.S. Geological Survey). 2008. "Mount Rainier—Living Safely With a Volcano in Your Backyard." <https://pubs.usgs.gov/fs/2008/3062/fs2008-3062.pdf>.
- USGS. 2016a. "Tsunami hazards—A National Threat." <https://water.usgs.gov/edu/tsunamishazards.html>. Accessed February 28, 2017.
- USGS. 2016b. "U.S. Volcanoes and Current Activity Alerts." <https://volcanoes.usgs.gov/index.html>. Accessed February 28, 2017.
- Vastag, B. 2011. Nuclear power plant remains offline after August earthquake. *The Washington Post*, November 1.
- Wuebbles, D., G. Meehl, K. Hayhoe, T.R. Karl, K. Kunkel, B. Santer, M. Wehner, et al. 2014. CMIP5 climate model analyses: Climate extremes in the United States. *Bulletin of the American Meteorological Society* 95(4): 571–583.

# 4

## Strategies to Prepare for and Mitigate Large-Area, Long-Duration Blackouts

### INTRODUCTION

This chapter focuses on strategies that can help to avoid, prepare for, and reduce the likelihood, magnitude, and duration of large-area, long-duration outages.<sup>1</sup> Although this report is predominantly concerned with large-scale outages, many of the preventative approaches described in this chapter also decrease the likelihood of small localized outages and can help limit the spread and impact of small disruptions before major recovery efforts (see Chapter 6) are required.

This chapter concentrates on two broad aspects of improving grid resilience, considering both physical and cyber impairments. The first, planning and design, describes actions to enhance resilience that can be taken well before a potentially severe physical or cyber event occurs. The second, operations, describes how the grid is operated and strategies to enhance resilience during a severe event. Certainly there is overlap between these two, and the dividing line can blur as the planning time horizon moves closer to the real-time world of operations.

### PLANNING AND DESIGN

The electric utility industry has a long history of planning, and the present high levels of reliability attest to its success in this area. However, the majority of this planning and design work has been directed toward increasing system reliability, while focusing on designing the system for optimal operations during normal conditions and creating the ability to respond to events similar to those that have been previously encountered by grid operators. Planning and design for resilience is different, with challenges that touch on essentially all aspects of the electric grid.

A resilient design requires a holistic consideration of both the resilience of the individual components that comprise

modern electric grids and the resilience of the system as a whole. There is, of course, overlap between the two: system resilience can be enhanced by improved component resilience. However, improved resilience also involves consideration of the system as a whole, including not just the electric infrastructure itself, but also the interdependent infrastructures such as natural gas infrastructure, support infrastructure for the supply of other key inputs, and the commercial communications systems used in operating the grid. Last, improved resilience requires regulatory consideration of how upgrades will be funded.

### Component Hardening and Physical Security

Creating reliable and secure components, investing in system hardening, and pursuing damage prevention activities are all strategies that improve the reliability of the grid and likewise play a role in preventing and mitigating the extent of large-area, long-duration outages. Utilities are generally aware of local hazards; however, these hazards may change over time, and utilities may not be aware of the compound vulnerabilities that become increasingly possible. Strategies used to address these hazards include appropriate design standards, siting methods, construction, maintenance, inspection, and operating practices. For example, a transmission line traversing high mountains must be designed for heavy ice loading, which may not be a design consideration for infrastructure located in desert environments. Design considerations for generation facilities, substations, transmission lines, and distribution lines frequently include environmental conditions such as extreme heat, cold, ice, and floods among other known threats. Utilities have less experience in design and hardening for uncommon threats such as geomagnetic disturbance (GMD) or electromagnetic pulse (EMP); nonetheless, these have been the focus of increasing attention and strategies to reduce system vulnerability.

Utility investment in system hardening is typically informed by a risk-based cost-performance optimization that strives to be economically efficient by investing in

<sup>1</sup> Such events overlap with what the North American Electric Reliability Corporation (NERC) calls a “severe event,” defined as an “emergency situation so catastrophic that complete restoration of electric service is not possible” (NERC, 2012a).

mitigation strategies with the greatest reduction in risk at the lowest cost (Figure 4.1). In principle, an infinite amount of money could be spent hardening and upgrading the system with costs passed on to ratepayers or taken from shareholder returns. However, utilities and their regulators (or boards) are typically conservative in these investments. All mitigation strategies have cost-performance trade-offs, and it may be difficult to estimate the actual reduction in risk or improvement in resilience associated with a specific action. In most cases, an electricity system that is designed, constructed, and operated solely on the basis of economic efficiency to meet standard reliability criteria will not be sufficiently resilient. If some comprehensive quantitative metric of resilience becomes available, it should be combined with reliability metrics to select a socially optimal level of investment. In the meantime, decision makers must employ heuristic procedures to choose a level of additional investment they believe will achieve a socially adequate level of system redundancy, flexibility, and adaptability.

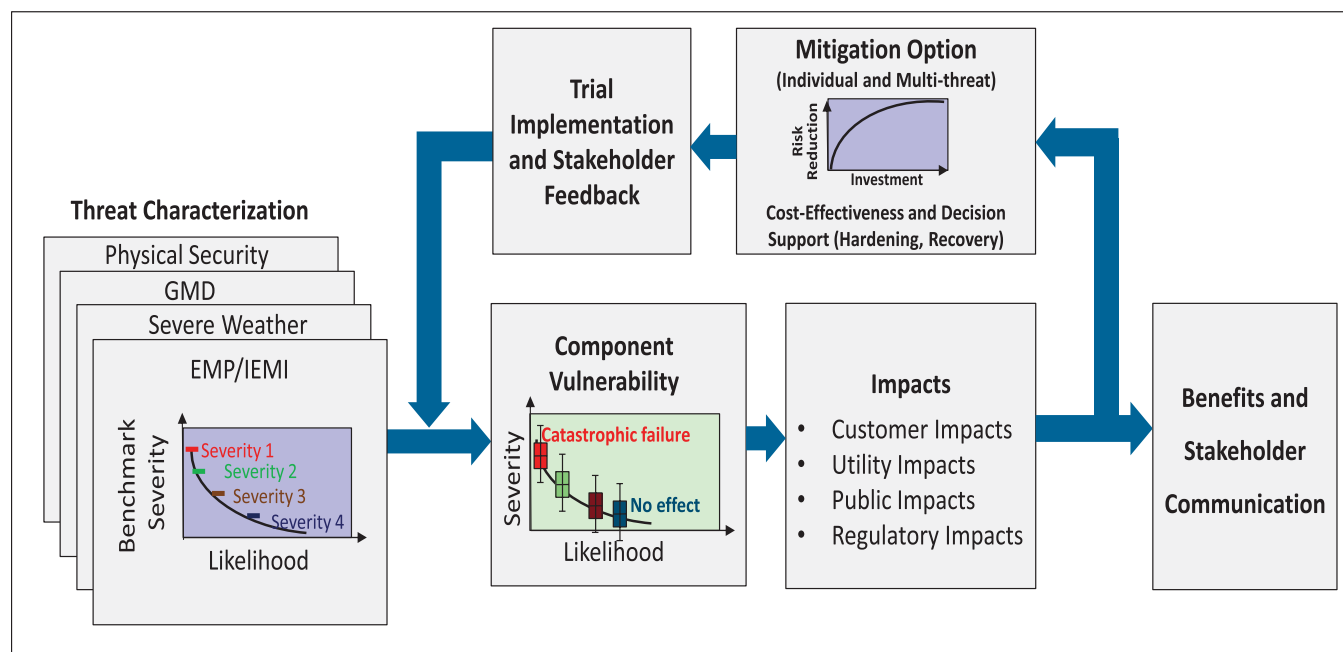
**Finding:** Design choices based on economic efficiency using only classical reliability metrics are typically insufficient for guiding investment in hardening and mitigation strategies targeted toward resilience. Such choices will typically result in too little attention to system resilience. If adequate metrics for resilience are developed, they could be employed to achieve socially optimal designs. Until then,

decision makers may employ heuristic procedures to choose the level of additional investment they believe will achieve socially adequate levels of system redundancy, flexibility, and adaptability.

Hardening and mitigation strategies can improve electricity grid reliability and resilience, and utilities routinely employ many techniques when deemed cost appropriate. Common examples are described in the following paragraphs.

### Vegetation Management

Many outages, particularly those in the distribution system, are caused by trees and vegetation that encroach on the right-of-way of power lines. Overhead transmission lines are not directly insulated and instead require minimum separation distances for air to provide insulation. If trees or objects are allowed to get too close and draw an arc, short circuits of the energized conductor can result. When they are heavily loaded, transmission line conductors heat up, expand, and sag lower into the right-of-way, which increases the likelihood of a fault at times of peak transmission loading. Therefore, inadequate vegetation management in transmission line rights-of-way is a common cause of blackouts. On the lower-voltage distribution system, separation requirements are much smaller, and line sag is less of a consideration. However, during high wind or icy conditions, falling trees



**FIGURE 4.1** The process of considering and mitigating individual component vulnerability based on cost-performance optimization.

NOTE: GMD, geomagnetic disturbance; EMP, electromagnetic pulse; IEMI, intentional electromagnetic interference.

SOURCE: Courtesy of the Electric Power Research Institute. Graphic reproduced by permission from the Electric Power Research Institute from presentation by Rich Lordan to the NCSL-NARUC Energy Risk & Critical Infrastructure Protection Workshop, Transmission Resiliency & Security: Response to High Impact Low Frequency Threats. EPRI, Palo Alto, Calif.: 2016.



and limbs can either create a short circuit or tear down the wires themselves. This can be extremely hazardous when the energized wires are in close proximity to people. So while there are different vegetation management practices for transmission (clearing vegetation below the wires) and distribution (clearing vegetation from around and above the wires), vegetation management is a key factor that influences the reliability of the transmission and distribution (T&D) system. Following the widely publicized blackout of August 14, 2003, new national standards for vegetation management of transmission lines were implemented. However, the vegetation management practices for distribution utilities vary dramatically, influenced by a variety of factors including geography, public sentiment, and regulatory encouragement.

### Undergrounding

Undergrounding of T&D lines is often more expensive than building aboveground infrastructure. Outside of dense urban environments, T&D assets are typically not installed underground unless land constraints, aesthetics, or other community concerns justify the cost. Undergrounding protects against some threats to the resilience of the electric grid, such as severe storms—a leading cause of outages—but it does not address all threats (e.g., seismic or flooding) and may even make recovery more challenging. Furthermore, undergrounding may be impractical in some areas, based on geologic or other constraints (e.g., areas with a high water table). Therefore, the decision of whether or not to underground T&D assets varies considerably based on local factors; while undergrounding may have resilience benefits in some circumstances, it does not offer a universal resilience benefit.

### Reinforcement of Poles and Towers

Building the T&D network to withstand greater physical stresses can help prevent or mitigate the catastrophic effects of major events. Structurally reinforcing towers and poles (referred to as robustness) is more common in areas where heavy wind or ice accumulations are possible, but the degree to which they are reinforced presents a cost trade-off with clear resilience implications.

### Dead-End Structures

To minimize cost, transmission towers are often designed to support only the weight of the lines, with lateral support provided by the lines themselves, which are connected to adjacent towers. Thus, if one tower is compromised, it can potentially create a domino effect whereby multiple towers fail. To limit this, utilities install dead-end structures with sufficient strength to stop such a domino effect. However, there is a cost trade-off associated with how often such structures should be installed (e.g., changing the spacing

from having one dead-end structure every 4 miles versus one dead-end structure every 10 miles).

### Water Protection

Flooding is often a greater concern for substations and generation plants than transmission and distribution lines, and storm surge is particularly challenging for some coastal assets. When siting new facilities, it is possible to avoid low lying and flood prone areas. There are, however, many legacy facilities located in high hazard areas. Given that much of the population lives in coastal areas, it is impossible to address this risk completely through siting alone. Common techniques include installing dikes and/or levees, if land permits, or elevating system components above flood levels, which can be expensive when retrofitting legacy facilities.

### Emerging Strategies for Geomagnetic Disturbance and Electromagnetic Pulse

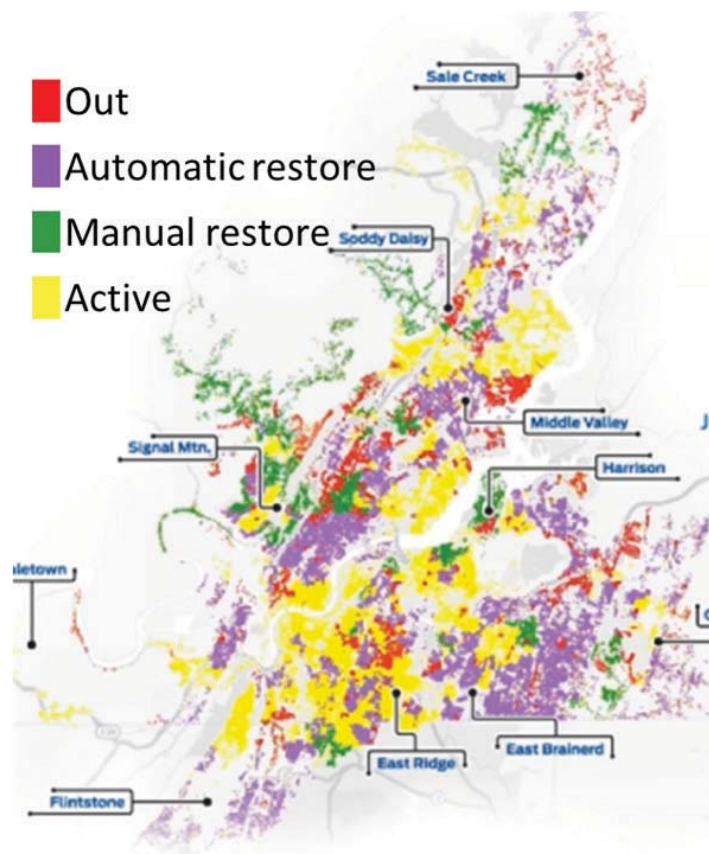
There are various electromagnetic threats to the power system, including GMD (naturally occurring) and EMP (man-made). Both of these threats have resilience considerations at the component level and from a system-wide perspective. While they have different mechanisms of coupling to the grid and inducing damage, they are similar in that they can damage high-value assets, such as transformers. The EMP threat is unique in that it can directly incapacitate digital equipment such as microprocessors and integrated circuits that are not military hardened. NERC has new planning requirements for mitigating GMD (NERC, 2016a), and various commissions (e.g., the Commission to Assess the Threat to the United States from Electromagnetic Pulse [EMP] Attack<sup>2</sup>) have explored the degree to which it is appropriate to harden civilian infrastructure to address the EMP threat.

### Physical Security

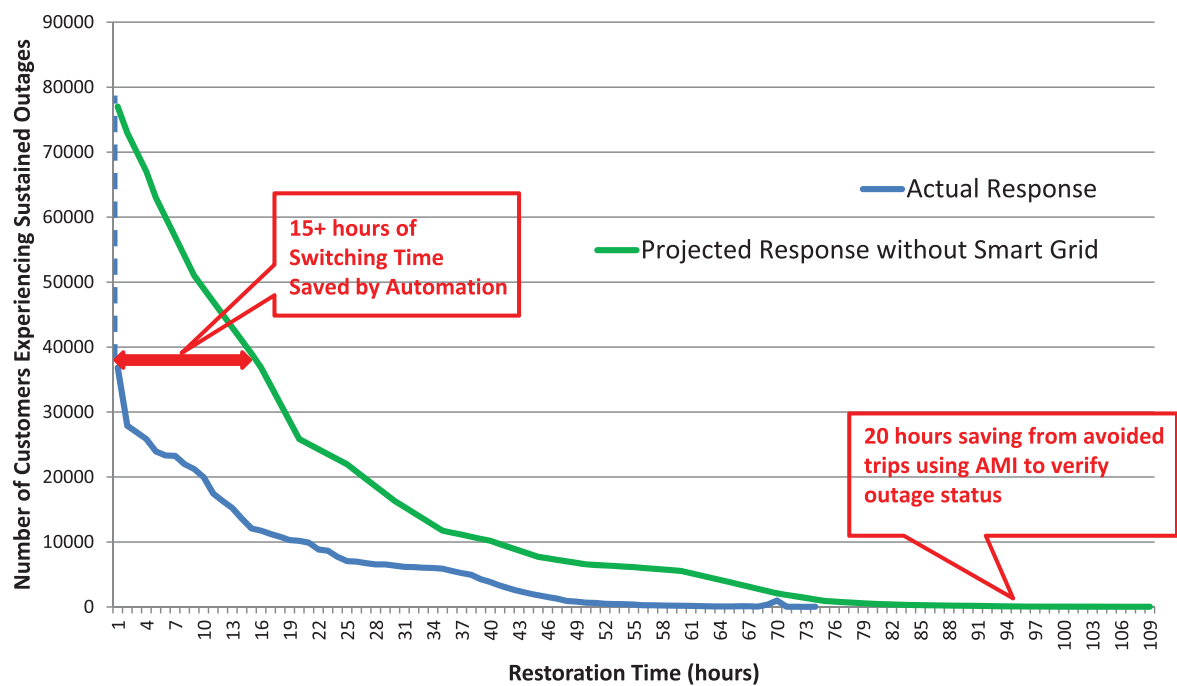
The immense size and exposed nature of electricity infrastructure makes complete physical protection from attacks impossible; thus, there is a spectrum of physical security practices employed across the grid. Utilities selectively protect critical system components, and NERC standard CIP-014-2 (NERC, 2014a) is enforced on the transmission system. Distribution systems are outside the scope of NERC jurisdiction. Because many generation facilities are staffed, they are relatively well protected. Additional federal requirements apply to protecting nuclear and other key assets, such as federally owned dams. Other assets essential to the operation of the system, such as control centers, can resemble bunkers and are well guarded. Many substations are

<sup>2</sup> Reports from the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack can be found at <http://www.empcommission.org>, accessed August 2, 2017.

(A)



(B)



**FIGURE 4.2** (A) Following a major storm that disrupted service on many distribution circuits operated by Chattanooga Electric Power Board, automatic reconfiguration prevented outages for many customers (purple) and significantly reduced the number of circuits requiring manual repairs (green); and (B) such automation has greatly reduced the number of customer-hours (area under the curve) of outage experienced. NOTE: AMI, advanced metering infrastructure. SOURCE: Glass (2016).



less protected and have only surveillance, locks, and other deterrents. However, historical events such as the Metcalf incident (see Box 3.1) and a recent “white hat” break-in and hack of a utility shared on YouTube call attention to the limitations of these strategies. Alternative strategies include redesigning substation layout to minimize exposure, deploying barriers, protecting information about the location of critical components, and improving adoption of best practices and standards (ICF, 2016). Examples of these practices learned from the Metcalf incident include greater emphasis on outside-the-fence measures, including camera coverage, lighting, and vegetation clearing.

### Distribution System Resilience

As noted in Chapter 2, the wires portion of the electric grid is usually divided into two parts: the high-voltage transmission grid and the lower-voltage distribution system. The transmission system is usually networked, so that any particular location in the system will have at least two incident transmission lines. The advantage of a networked system is that loss of any particular line would not result in a power outage. In contrast, the typical distribution system is radial (i.e., there is just a single supply), although networked distribution systems are often used in some urban areas (NASEM, 2016a). Most aspects of resilience to severe events ultimately involve the transmission system; however, improved distribution system resilience can play an important role.

There is wide variation in the level of technological sophistication in distribution systems. The most advanced distribution utilities have dedicated fiber-optic communications networks, are moving away from the traditional radial feeder design toward more networked architectures, and have sectionalizing switches that allow isolation of damaged components. In response to damage on a distribution circuit, these systems automatically reconfigure the distribution network to minimize the number of customers affected. In one notable example, shown in Figure 4.2 and detailed in Box 4.1, the Chattanooga Electric Power Board (EPB) installed significant distribution automation technology with a \$111 million grant from the Department of Energy (DOE) through its Smart Grid Investment Grant program (authorized by the 2009 American Recovery and Reinvestment Act). The sophisticated and extensive project entailed installing a dedicated fiber-optics communications system, smart distribution switches, advanced metering infrastructure, and other equipment to automate restoration (DOE, 2011). It decreased restoration times for EPB’s customers, increased savings to EPB, and demonstrated possibilities for other utilities to emulate. However, pursuing a closed-loop fiber-optic system may be a challenge in other utility service areas that are larger geographically and in terms of population. While fiber-optic communication offers an advantage, it is not required to integrate the other technologies used at EPB. However, the deployment of a fiber-optic system lays the foundation

#### BOX 4.1 Financial and Operational Benefits of Distribution Automation to Chattanooga Electric Power Board

**Resilience and Reliability:** The installed fiber-optic network allows EPB to manage a greater number of restoration crews following a storm event and, based on a limited time frame, improve its system average interruption duration index (SAIDI) and system average interruption frequency index (SAIFI) reliability metrics (Glass, 2016; Wade, 2016).

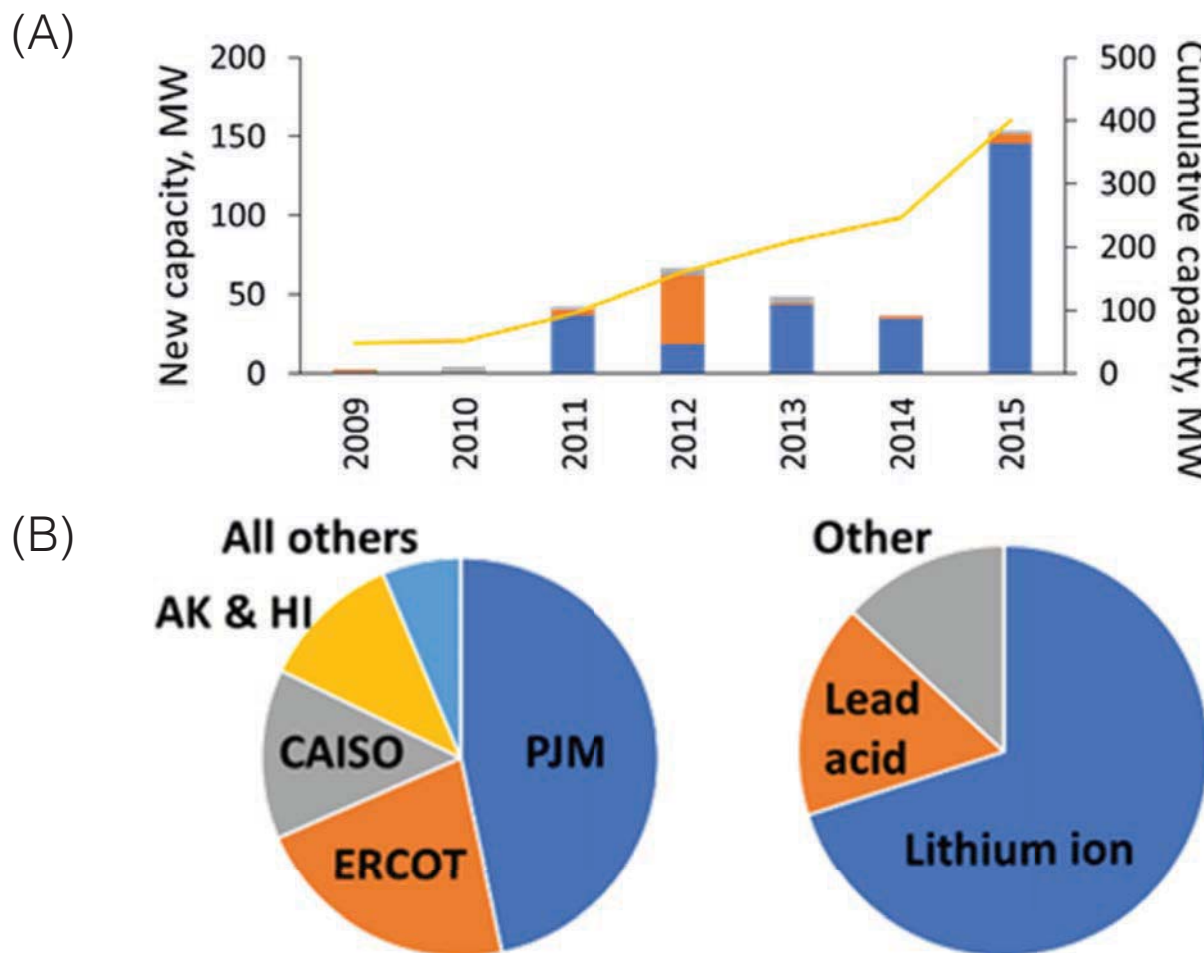
**Financial Savings:** Annual savings of \$200,000 are due to decreased dispatch of restoration crews, \$2.5 million from automated meter reading and remote disconnect, and \$2.7 million in energy demand savings from demand response and voltage control. Taken together, EPB saves nearly \$5.5 million as a result of its fiber-optic and automation technologies (Glass, 2016).

for technologies that result in very high data exchange rates, such as phasor measurement units (PMUs), and offers the ability to provide broadband access to the community.

A distribution fault anticipation application based on “waveform analytics” (Wischkaemper et al., 2014, 2015) is another example of a technology that could be applied today. The key idea behind this approach is to utilize fast sensing of the distribution voltages and currents to detect precursor waveforms, which indicate that a component on a distribution circuit will soon fail. This is in contrast to the traditional approach of waiting for the component to fail and cause an outage before doing repairs. Examples of problems that can be detected by such pre-fault waveform analysis include cracked bushings, pre-failure of a capacitor vacuum switch, fault-induced conductor slap (in which a fault current in the distribution circuit induces magnetic forces in another location, causing the conductors to slap together), and pre-failure of clamps and switches.

**Finding:** While many distribution automation technologies are available that would enhance system resilience, their cost of deployment remains a barrier, particularly in light of challenges in monetizing the benefits of such installations.

**Recommendation 4.1:** Building on ongoing industry efforts to enhance system resilience, the Department of Energy and utility regulators should support a modest grant program that encourages utility investment in innovative solutions that demonstrate resilience enhancement. These projects should be selected to reduce barrier(s) to entry by improving



**FIGURE 4.3** (A) Installations of utility-scale battery storage have increased substantially over the past 5 years, (B) although growth is concentrated in a few areas and dominated by lithium-ion chemistries.

NOTE: CAISO, California Independent System Operator; ERCOT, Electric Reliability Council of Texas.

SOURCE: Data from Hart and Sarkissian (2016).

regulator and utility confidence, thereby promoting wider adoption in the marketplace.

### Utility-Scale Battery Storage

Utility-scale battery storage is a relatively new tool available to operators to manage power system stability, which can potentially help prevent or mitigate the extent of outages. Of course even large batteries can only supply power for periods of hours, but such systems have value in other ways. They can be used to dispatch large amounts of power for frequency regulation, potentially preventing propagation of system disturbances, and provide additional flexibility for managing stability in lieu of demand response or load shedding. Installations of large utility-scale batteries (as opposed to behind-the-meter batteries) have increased significantly in several regions of the United States over the past 5 years. The DOE Global Energy Storage Database has information

on more than 200 utility-scale battery projects in the United States, with more than 400 MW installed or approved capacity by the end of 2015 (Figure 4.3) (Hart and Sarkissian, 2016). This data set may underestimate such storage capacity.<sup>3</sup> Other areas leading installation are in the Electric Reliability Council of Texas (ERCOT) and in California, driven largely by state policies (NREL, 2014). The small (relative to the scale of the three North American interconnections) Railbelt Electric System in Alaska was an early adopter (2003) of utility-scale battery energy storage, in part owing to instability challenges associated with operating a small, low-inertia “islanded” grid. Most utility-scale batteries on the grid employ lithium-ion chemistry and are used primarily for power conditioning and, to a lesser extent, for peak load management. Lithium-ion chemistry using existing electrolytes

<sup>3</sup> The committee believes there is approximately 400 MW capacity installed in the PJM service territory alone.

is not ideal for bulk storage of electricity from large-scale, variable renewable generation sources, but alternative battery chemistries have yet to reach the cost, performance, and manufacturing scale to impact utility operations.

### **Distributed Energy Resources**

Distributed energy resources (DERs)—including distributed generation from photovoltaics, diesel generators, small natural gas turbines, battery storage, and demand response—have the potential to help prevent the occurrence of large-area, long-duration outages as well as to provide local power to critical services during an outage. In California, for example, storage aggregators are contracting with utilities to provide tens of MW of storage capacity—alongside 70 MW of utility-scale storage—to help manage local resource adequacy and reliability following the closure of the Aliso Canyon facility (see Box 4.2). However, the reliability and resilience benefits of DERs to the bulk power system vary significantly, based on their technical characteristics and capacities as well as their location and local grid characteristics. Historically, DER adoption has

been driven by environmental considerations and consumer preferences; only recently has resilience become an explicit design consideration. The greatest resilience benefits can be realized through coordinated planning and upgrading of T&D systems, as well as by providing operators the ability to monitor and control the operating characteristics of DERs in real time and at scale. This may require changes to technical standards, regulations, and contractual agreements.

Strategically placed DERs (that are visible to and controllable by utilities) not only provide local generation at the end of vulnerable transmission lines, but also can be operated to relieve congestion and potentially avoid the need for new transmission infrastructure. Thus, some of the early applications of DERs for enhanced resilience were motivated by local system concerns—in locations with constraints on transmission expansion or at the end of lines that are known to be problematic.

### **Inverter Standards for Increased Visibility and Control**

At current levels of installation (relatively low except in certain areas such as Hawaii), DERs are not likely to be used

## **BOX 4.2**

### **Examples of Electric System Vulnerability to Disruptions in Natural Gas Infrastructure**

#### **February 2011 Texas Freeze**

Abnormally cold temperatures across Texas and the southwestern United States caused many natural gas well heads to freeze, which in turn resulted in curtailment of natural gas deliveries to end-use customers and, to a lesser extent, natural gas fired power plants. The cold weather caused 193 power plants (with cumulative load of nearly 30,000 MW) in ERCOT to fail to start or to be de-rated because of frozen equipment, blade icing, and low temperature cutoff limits. At the worst point in the event, one-third of the total ERCOT generator fleet was unavailable. System operators resorted to shedding load and instituted rolling blackouts to prevent an ERCOT-wide uncontrolled blackout. Although electricity–natural gas interdependency was not the primary cause of lost electric load or curtailed natural gas deliveries, the growing interdependency did contribute to the problem (NERC, 2011).

#### **January 2014 Polar Vortex**

In January 2014, a mass of cold air moved south across much of the country, plunging the Midwest, Northeast, and Southeast into temperatures 20° to 35° colder than average. The cold snap resulted in above average demand for electricity and natural gas for home heating. Many natural gas power plants were unable to operate as natural gas deliveries were curtailed, and grid operators had to resort to shedding interruptible load to maintain service. Less than 50 MW of firm load was shed over several days, and the event was handled effectively in part because of training and preparation. However, the event focused attention on the vulnerability associated with increasing reliance on natural gas for electricity restoration. Following the 2014 Polar Vortex, NERC made a number of recommendations for operators to increase awareness and coordination with natural gas suppliers, markets, and regulators (NERC, 2014b).

#### **October 2015 Aliso Canyon Storage Facility Closure**

A major gas leak was detected in the Aliso Canyon natural gas storage facility in October 2015, resulting in the facility's closing in early 2016. As the second largest natural gas storage facility in the United States, Aliso Canyon supplied gas to 18 power plants in the Los Angeles area with a total generation capacity near 10,000 MW (NERC, 2016b). Analysis suggests that closure of the facility may have significant electricity system reliability impacts, as well as curtailment of gas deliveries, in both summer and winter (CEC, 2016). In combination with the 2014 Polar Vortex, the Aliso Canyon blowout prompted the industry to undertake additional planning and risk mitigation strategies to reduce the likelihood that outages will result from natural gas system constraints.

explicitly for the purpose of preventing or mitigating large-scale outages. Nonetheless, as DER installations continue to grow, it may become possible to coordinate their dispatch to help prevent outages (i.e., maintain system stability) and to expedite restoration (as described in Chapter 6). However, realizing these system benefits would require that system operators—whether distribution utilities or independent parties—have visibility and an appropriate level of control over the majority of DERs in a region.

This will require changes in interconnection standards, notably regarding inverters that are the interface between many types of DERs and the distribution system. In the past, these standards, which are under revision as of this writing, have required that DERs disconnect from the grid under fault conditions. This is undesirable behavior because it can jeopardize system stability under significant DER penetration levels. In the revised standards (IEEE, 2017), inverters will be required to ride through grid events, and they will have the ability to provide voltage and frequency regulation. Future inverters will provide operators with updated information on DER performance (e.g., generation level, state of charge), who could in turn actively utilize these resources in running the grid (e.g., when implementing adaptive islanding or intelligent load shedding schemes).

A non-exhaustive list of advanced inverter functionalities that could help prevent or mitigate outages, if they can be leveraged at scale, includes the following:

- *Frequency-watt function.* Adjusts real power output based on service frequency and can aid in frequency regulation during an event.
- *Volt-var and volt-watt function.* Adjusts reactive and/or real power output based on service voltage; this is necessary to maintain distribution feeder voltages within acceptable bounds when DER penetration is high, but it could also be used for transmission-level objectives.
- *Low/high voltage and frequency ride-through.* Defines voltage and frequency ranges for the inverter to remain online during a disturbance, which becomes a key feature at high DER penetration levels.
- *DER settings for multiple grid configurations.* Enables a system operator to provide a DER with alternate settings, which may be needed when the local grid configuration changes (e.g., during islanding or circuit switching).

**Finding:** DERs have a largely untapped potential to improve the resilience of the electric power system but do not contribute to this inherently. Rather, resilience implications must be explicitly considered during planning and design decisions. In addition, the possibility exists to further utilize DER capabilities during the operational stage.

**Recommendation 4.2:** The Department of Energy and the National Science Foundation, in coordination with state

agencies and international organizations, should initiate research, development, and demonstration activities to explore the extent to which distributed energy resources could be used to prevent large-area outages. Such programs should focus on the technical, legal, and contractual challenges to providing system operators with visibility and control over distributed energy resources in both normal and emergency conditions. This involves interoperability requirements and standards for integration with distribution management systems, which are ideally coordinated at the national and international levels.

### Interconnected Electric Grid Modeling and Simulation

From the start of the power industry in the 1880s, modeling and simulation have played a crucial role, with much expertise gained over this time period. Over the past 60 years or so, much of this expertise has been embedded in software of increasing sophistication, with power-flow, contingency-analysis, security-constrained optimal power-flow, transient-stability, and short-circuit analysis some of the key modeling packages (NASEM, 2016b). Modeling and simulation occur on time frames ranging from real time, in the case of operations, to looking ahead for multiple decades when planning high-voltage transmission line additions.

While the tools are well established for these traditional applications, enhancing resilience presents some unique challenges. First, multidimensional modeling is needed because severe events are likely to affect not just the electric grid, but also other infrastructures. Second, in order to enhance resilience, simulations should be specifically designed to consider rare events that severely stress the grid. Many rare high-impact events will stress the power grid in new and often unexpected ways; as a consequence, most will also likely stress the existing power system modeling software. The degree of power system impact often requires detailed modeling of physical and/or cyber systems associated with the initiating event. For example, correctly modeling the impacts of large earthquakes requires coupled modeling between the power grid and seismic simulations (Veeramany et al., 2016). This requires interdisciplinary collaboration and research between power engineers and people from a potentially wide variety of different disciplines. On the cyber side, for example, one must be able to correctly model the occurrence, nature, and impact of a large-scale distributed cyber attack like the one in Ukraine in 2015.

Because such events are rare, there is typically little or no historical information to accurately quantify or characterize the risk: some of the more extreme events could be considered extreme manifestations of more common occurrences (NASEM, 2016b). Thus, a large-scale attack could be considered a more severe manifestation of the more regular disturbances (such as those due to the weather). However, others would be more novel. As an example, consider the modeling and simulation work being done to



study the impact of GMD on the power grid. GMDs, which are caused by coronal mass ejections from the sun, cause low frequency ( $\ll 0.1$  Hz) variations in the earth's magnetic field. The changing magnetic field can then induce electric fields on the earth's surface that cause quasi-direct current geomagnetically induced currents to flow in the high-voltage transmission system, potentially causing saturation in the high-voltage transformers. A moderate GMD, with a peak electric field estimated to be about 2 V/km, caused a blackout for the entire province of Québec, Canada, in 1989 (Boteler, 1994), while much larger GMD events occurred in North America in 1859 and 1921.

As noted by Albertson et al. (1973), the potential for GMD to interfere with power grid operations has been known at least since the early 1940s. However, power grid GMD assessment is still an active area of research and development; much of that work has occurred in the past few years through interdisciplinary research focusing not just on the power grid, but also on the sun, the earth's upper atmosphere, space weather hazards, and the earth's geophysical properties. The assumptions on modeling the driving electric fields in software have evolved from a uniform electric field (NERC, 2012b); to scaled uniform direction electric fields, based on ground conductivity regions (based on one-dimensional earth models) (NERC, 2016a); to varying magnitude and electric fields, based on three-dimensional earth models using recent National Science Foundation Earthscope results (Bedrosian and Love, 2015). Over the past few years, GMD analysis has been integrated into commercial power system planning tools including the power flow (Overbye et al., 2012) and transient stability analysis software (Hutchins and Overbye, 2016).

Determining the magnitudes of the severe events to model can be challenging since there is often little historical record. This was highlighted in 2016 by the Federal Energy Regulatory Commission (FERC) in their Order 830,<sup>4</sup> which directed NERC to modify its Standard TPL-007-1 GMD benchmark event so as not to be solely based on spatially averaged data. The challenges of using measurements of the earth's magnetic field variation over about 25 years to estimate the magnitude of a 100-year GMD are illustrated by Rivera and Backhaus (2015). Determining the scenarios to consider for human-caused severe events, such as a combined cyber and physical attack, are even more challenging.

**Finding:** Enhancing power grid resilience requires being able to accurately simulate the impact of a wide variety of severe physical events and malicious cyber attacks on the power grid. Usually these simulations will require models for either coupled physical and cyber infrastructures or physical systems. There is a need both for basic research on the nature of these simulations and applied work to develop adequate simulations to model these severe events and malicious cyber attacks.

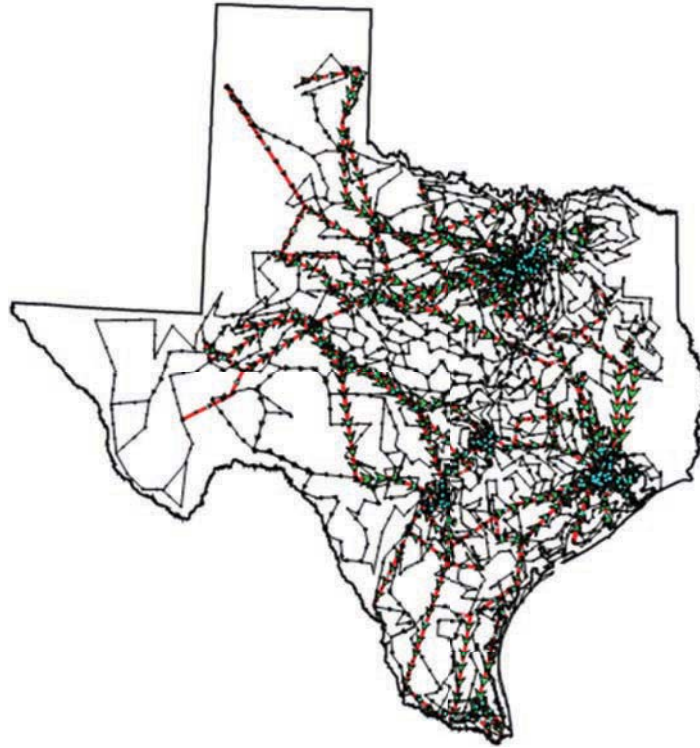
**Recommendation 4.3:** The National Science Foundation should continue to expand support for research looking at the interdisciplinary modeling and mitigation of power grid severe events. The Department of Energy should continue to support research to develop the methods needed to simulate these events.

A key driver for the research and development of simulation tools for improved resilience is access to realistic models of large-scale electric grids and their associated supporting infrastructures, especially communications. Some of this information was publicly available in the 1990s, but, as a result of the Patriot Act of 2001, the U.S. electric power grid is now considered critical infrastructure, and access to data has become much more restricted. While some access to power grid modeling data is available under non-disclosure agreements, these restrictions greatly hinder the exchange of the models and results needed for other qualified researchers to reproduce the results. This need is particularly acute for resilience studies, in which models need to be shared among researchers in a variety of fields for interdisciplinary work.

A solution that protects critical infrastructure information is to create entirely synthetic models that mimic the complexity of the actual grid but contain no confidential information about the actual grid. Such models are now starting to appear, driven in part by the DOE Advanced Research Projects Agency-Energy Grid Data program (ARPA-E, 2016), which is focused on developing realistic, open-access power grid models primarily for use in the development of optimal power flow algorithms. A quite useful characteristic of such synthetic models would be to include realistic geographic coordinates in order to allow the coupling between the power grid and other infrastructures or the actual geography. Birchfield et al. (2016) suggest using an electric load distribution that matches the actual population in a geographic footprint, public data on the actual generator locations, and algorithms to create an entirely synthetic transmission grid. As an example, Figure 4.4 shows a 2000-bus entirely synthetic network sited geographically in Texas. The embedding of geographic coordinates with the existing Institute of Electrical and Electronics Engineers' 145-bus test system is used by Veeramany et al. (2016) to present a multi-hazard risk-assessment framework for study of power grid earthquake vulnerabilities.

While there has been some progress in creating synthetic models for the physical side of the electric grid, there has been very little progress in creating realistic models for the communications that support grid operations, both to represent its complexity and extent and to represent its coupling with the physical portion of the grid. Such models are necessary to understand the overall resilience of the power grid. Without such models, it is impossible to understand the impact of a cyber attack on the physical portion of the grid and hence its ability to deliver power despite a cyber attack.

<sup>4</sup> 156 FERC ¶ 61,215.



**FIGURE 4.4** 2000-bus synthetic network sited in Texas. The red lines show 345 kV transmission lines, the black lines show 115 kV lines, and the green arrows show the flow of power from the generators to the loads.

SOURCE: © 1969 IEEE. Reprinted, with permission, from *Power Systems, IEEE Transactions on Grid Structural Characteristics as Validation Criteria for Synthetic Networks*.

**Finding:** A key objective for research and development of simulation tools for improved resilience is shareable access to realistic models of large-scale electric grids, considering both the grid's physical and cyber infrastructure and, equally important, the coupling between the two infrastructure sides. Because the U.S. power grid is considered critical infrastructure, such models are not broadly available to the power systems research community. Therefore, there is a need to develop synthetic models of the power grid physical and cyber infrastructure that match the size and complexity of the actual grid but contain no confidential information and hence can be fully publicly available.

**Recommendation 4.4:** The Department of Energy should support and expand its research and development on the creation of synthetic power grid physical and cyber infrastructure models. These models should have geographic coordinates and appropriate cyber and physical model detail to represent the severe events needed to develop algorithms to model and enhance resilience.

### Interconnected Electric Grid Planning

Planning for resilience requires providing sufficient redundancy in generation, transmission, and distribution capacity. Current reliability standards issued by NERC (that

are mandatory for operators of the bulk electricity system) require that the transmission system have enough redundant paths to withstand an outage by one major line or other important component (NERC, 2005). In most cases, the transmission system can continue operating with the loss of several transmission lines. At the distribution level, some state public utility commissions provide performance-based incentives that encourage distribution utilities to improve reliability metrics such as SAIDI and SAIFI, although these measures do not typically include outages associated with major events. Although NERC standards have largely been effective in addressing credible contingencies and have been recently expanded to include consideration of extreme events,<sup>5</sup> designing the grid to ride through catastrophic events such as major storms and cyber attacks pushes their limit. Furthermore, designing and building the system to withstand such major events is expensive, and while the electricity system is designed to be economically efficient (subject to reliability-based constraints such as adequacy requirements in design and operational contingency requirements in operation), additional analyses and changes in

<sup>5</sup> NERC TPL-001-4 requires studies to be performed to assess the impact of the extreme events; if the analysis concludes there is a cascading outage caused by the occurrence of extreme events, an evaluation of possible actions designed to reduce the likelihood or mitigate the consequences of the event(s) must be conducted (NERC, 2005).



planning, operational, and regulatory criteria may be needed to build incentives to design, plan, and operate the system to consider resilience in a cost-effective manner. Pushed too far, traditional strategies to make the system more robust can become cost-prohibitive, so planning and designing for graceful degradation and rapid recovery has become increasingly important for utilities.

With respect to transmission system level generation planning, the reliability standard followed in North America is a loss of load probability (LOLP) of 1 day in 10 years—enough generation capacity available to satisfy the load demand 99.97 percent of the time. If one can predict the maximum yearly load demand over many years, and good statistics of the central generator outage rates are available, one can calculate the schedule and amount of new generation capacity construction to meet this level of reliability.

As growing amounts of intermittent solar power have been added to distribution systems, the central plant generator models used in the traditional generation planning studies may be inadequate. The availability statistics were either unavailable or inadequate as the technologies were evolving. If the availability of demand curtailment, which is the same as generation availability, is also considered, the model for that will again be different, as this is dependent on factors other than weather. Finally, the addition of storage requires models that are even more complicated, as these can behave as either loads or generation with their own optimal charge/discharge schedules.

Although the generation planning criterion of the LOLP being 1 day in 10 years assures that the available generation capacity exceeds the load demand, the process ignores whether the transmission grid can move the generation to the load centers. The transmission planning process assures this by running power flow and transient stability studies on scenarios of extreme loading of the transmission grid. The planning criterion is that the system would operate normally (i.e., without voltage and loading violations) even if one major piece of equipment (e.g., line, transformer, generator) is lost for any reason—this is known as the “N-1” criterion.<sup>6</sup> Note that this is a worst case deterministic criterion, not a probabilistic criterion like LOLP; this is because no one has yet found a workable stochastic calculation that can compute the probability of meeting all the operational constraints of the grid.

These generation planning requirements work well for scenarios where there are a few central generator stations but if meeting the generation reliability requires the availability of the DERs on the distribution side (including demand and storage management), then it is not enough to run studies on only the transmission system. On the other hand, modeling

the vast numbers of distribution feeders into the contingency analysis studies would increase the model sizes by at least one magnitude. Even though this may not pose a challenge to the new generation of computers, it does pose a huge challenge to the present capabilities of gathering, validating, exchanging, and securing the model data.

The decision to invest in new generation, transmission, and distribution is more impacted by cost considerations where reliability objectives are otherwise being met. The least cost consideration must take into account not just the capital cost, but also the operational cost over the lifetime of the generation, transmission, or distribution. This cost optimization process has to include the operational scenarios over several decades, resulting in a dynamic optimization.

A major procedural hurdle has been the fact that generation (and even transmission, which is regulated) can be built by third parties whose optimal decision may or may not coincide with the optimal decision for the whole system. This multi-party decision making has essentially made the process much more difficult, and there is concern that the present decision making is too fragmented to guarantee the needed robustness of the future grid.

It is difficult enough to include all of the control and protection that is part of the grid today, but the use of distributed generation, demand response, and storage will require much more control and protection. Moreover, the rapid deployment of better measurement (advanced metering infrastructure, distribution management systems, and phasor measurement units) and communication (fiber optics) technologies are enabling a new class of control and protection that are not yet embedded into commercial-grade simulation packages.

### **Architectural Strategies to Reduce the Criticality of Components**

A reliable system includes reliable components and a system architecture design that reduces the criticality of individual components needed to maintain grid functionality. A redundant and diverse architecture can enhance resilience of the system by reducing the dependencies on single components and how they contribute to the overall system objectives. Considerations of cascading failures, fault tolerant and secure system design, and mutual dependencies are important to develop resilient architectures. While many design characteristics of the modern power grid employ these concepts, it is important to improve resilient architecture design principles to enhance the capability of the system and to have a high degree of operational autonomy under off-normal conditions.

Historically, one of the primary means of achieving system resilience in the event of accidental component failure is through redundancy. This approach has been adopted by the electricity industry since its inception and has served

<sup>6</sup> The N-1 criterion, referring to surviving the loss of the single largest component, is shorthand for a more complex set of NERC standards that specify the analysis of various categories of “credible contingencies” and acceptable system responses.

the customers well. For particularly important components or subsystems, this redundancy can also include diversity of design so as to prevent common mode failures or deliberate attacks from compromising both the primary and secondary components. Both redundancy and diversity in design are often employed in communication networks.

In addition, there is a need to design systems with insights provided by simulation of cascading failure sequences, so that technical or procedural countermeasures to thwart cascading failure scenarios can be applied. This preemptive analysis (and configuring the system to avoid conditions where cascading failure is a credible outcome) is particularly important because the speed of cascading failure sequences can often exceed the capability of automatic control responses, especially when the wide-area nature of the grid, and inherent communication delays, are taken into account.

One approach of resilient system design is to install controls that respond appropriately to limit the consequences or even stop a cascading failure sequence, regardless of the specific scenario that initiated the event. Thus, the system remains resilient even if events occur that are not envisioned or beyond the design basis of the system. Under-frequency load shedding is a notable example of this type of control. It operates when the system is in distress, and the resulting action of this control serves to help bring the system back into equilibrium. This design is elegant in that it is always appropriate to shed load when the system is experiencing a prolonged low frequency condition and that these controls can be autonomous and isolated, making them very secure and robust. Therefore, the presence of this type of control helps to enhance resilience, independent of the specific scenario or sequence of events that led up to its activation. Future implementation of under-frequency load shedding schemes will need to take into account the number of DERs on distribution feeders. These schemes may need to rely on intelligent load shedding instead of disconnecting entire distribution feeders.

### Intelligent Load Shedding

Automatic under-frequency load shedding is a common strategy designed into systems, which maintains the stability of the grid when there is an unanticipated loss of generation. Load shedding events typically impact entire circuits, with all customers on the circuit losing power (NERC, 2015). However, with increasing deployment of advanced metering infrastructure (AMI) and sectionalizing switches on distribution systems, opportunities exist to significantly improve the precision and reduce unwanted outages associated with load shedding events. In the near future, it may be possible for utilities to disconnect specific meters on a distribution circuit as opposed to disconnecting the entire circuit at the substation. Some AMI provide greater granularity in control, allowing fractional supply as opposed to only full or no supply. Load shedding could be made even more selective with

the installation of “smart” circuit breakers within customer facilities that would disconnect specific circuits within a residence or facility, based on providing appropriate financial incentives to customers. This could be done automatically, as a function of parameters like frequency, or it could be done under a systems optimization controller, but these different levels of functionality have differing levels of communication requirements.

**Recommendation 4.5:** The Department of Energy, working with the utility industry, should develop use cases and perform research on strategies for intelligent load shedding based on advanced metering infrastructure and customer technologies like smart circuit breakers. These strategies should be supported by appropriate system studies, laboratory testing with local measurements, and field trials to demonstrate efficacy.

### Adaptive Islanding

The process of “islanding” the grid—that is, where the interconnection breaks up or separates into smaller, potentially asynchronous portions—can result in significant outages if the islanding is the result of an uncontrolled cascading failure. However, there are opportunities to pre-plan and manage the islanding process such that outages impact significantly fewer customers. Adaptive islanding can preserve the benefits of large-scale interconnected system operations during normal conditions while reducing the risk of failures propagating across the grid during abnormal or emergency conditions.

Under normal system conditions, the track record of system protection is excellent. But performance during off-normal conditions is less predictable. When a cascading failure progresses through a power system, the individual tripping of transmission lines will often result in the formation of islands. The stability of an island post-disturbance depends predominantly on the balance of generation and load within the area and the ability to maintain that balance during the sequence of events leading up to, during, and after island formation. Generator protection might act to trip unit(s) to prevent damaging transients. The nature of these transients and their severity, and the ability of the remaining generation to match the load within the island, will determine whether the island will be stable. Other emergency controls, such as automatic under-frequency load shedding, are useful to help preserve the stability of an island as it is being formed. The goal of under-frequency load shedding is preventing the loss of generation from under-speed protection. Losing generation due to over-speed protection is less consequential because high frequency is the result of too much generation in the first place. Usually, one good indicator of whether an island will survive or fail is whether that region of the system was a net exporter or a net importer of power prior to the disturbance. It is easier for generation to throttle down than to

throttle up, although under-frequency load shedding schemes can also be used to maintain stability within the island.

Wide-area protection schemes have been developed to limit the consequences of an uncontrolled cascading failure (NERC, 2013). These remedial action schemes provide fast-acting control to preserve system stability in response to predefined contingencies. One such scheme deliberately separates the western power system into two islands by remotely disconnecting lines in the eastern portion of the system if key transmission paths in the western portion of the system become de-energized.

Adaptive islanding is an idea that has been under development for several years (You et al., 2004). The concept is predefining how to break apart the system in response to system events, by matching clusters of load and generation. The goal is to reduce the size of power system blackouts, and minimizing generation loss is a key element of this strategy. This can be accomplished through more aggressive use of fast-acting demand response to preserve the generation-load balance in each of the islands. The technology has progressed to the point where this is becoming a viable approach.

**Finding:** The electricity system, and associated supporting infrastructure, is susceptible to widespread uncontrolled cascading failure, based on the interconnected and interdependent nature of the networks.

**Recommendation 4.6:** The Department of Energy should initiate and support ongoing research programs to develop and demonstrate techniques for degraded operation of electricity infrastructure, including supporting infrastructure and cyber monitoring and control systems, where key subsystems are designed and operated to sustain critical functionality. This includes fault-tolerant control system architectures, cyber resilience approaches, distribution system interface with distributed energy resources, supply chain survivability, intelligent load shedding, and adaptive islanding schemes.

### Vulnerability Due to Interdependent Infrastructures

A reliable electric grid is crucial to modern society in part because it is crucial to so many other critical infrastructures, as described in Chapter 2. However, the dependency goes both ways, as the reliable operation of the grid depends on the performance of multiple supporting infrastructures. Outages can be caused by disruptions to natural gas production and delivery, commercial communications infrastructure, and transportation systems, among other critical infrastructures (Figure 4.5) (Rinaldi et al., 2001).

### Natural Gas Infrastructure

As described in Chapter 2, the fraction of generation provided by natural gas—both large central generating plants and small customer-owned generators powered by

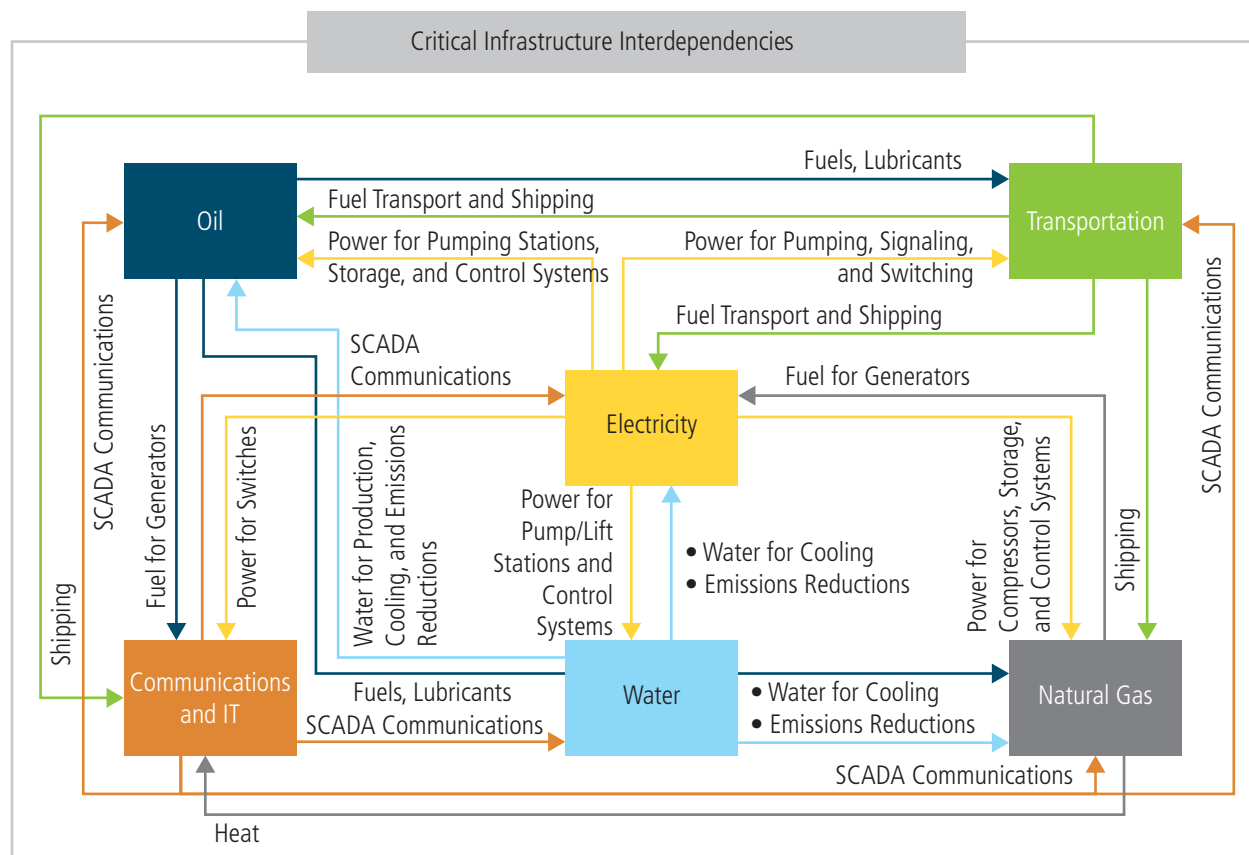
internal combustion motors or microturbines—has grown substantially over the past few years. This not only exposes the industry to potential price volatility and supply chain vulnerability, but also raises the question of how utilities could restore electricity service if a major disruption to natural gas delivery occurred (e.g., one or more critical pipelines are destroyed). To date, no such outage has resulted in large electricity outages, and the minor events that have occurred fall on the scale of reliability operations that were handled relatively easily by the industry. The January 2014 Polar Vortex and the natural gas leak and subsequent closing of Aliso Canyon natural gas storage facility have already impacted utility planning and system design to be more cognizant of this critical interdependency (Box 4.2). These studies suggest that resilience can be enhanced through a diverse fuel portfolio, where a single interruption is less likely to impact a significant number of generators that cannot be overcome by reserve assets.

**Finding:** Constraints in natural gas infrastructure have resulted in shedding of electric load, and the growing interdependency of the two systems poses a vulnerability that could lead to a large-area, long-duration blackout.

**Recommendation 4.7:** The Federal Energy Regulatory Commission and the North American Energy Standards Board, in conjunction with industry stakeholders, should further prioritize their efforts to improve awareness, communications, coordination, and planning between the natural gas and electric industries. Such efforts should be extended to consider explicitly what recovery strategies should be employed in the case of failed interdependent infrastructure. Fuel diversity, dual fuel capability, and local storage should be explicitly addressed as part of these resilience strategies.

### Commercial Communications Infrastructure

Another example of coupled infrastructure is telecommunications. While many utilities utilize their own dedicated telecommunication assets to support critical communication and automation functions, there is a substantial dependency on communications and internet-based technologies that facilitate the daily operation of the modern electricity system, including coordination among personnel, managing markets, and financial structures, as well as supporting automation and control technology. With growing deployment of smart grid technologies and automated controls, this dependency may continue to increase. In the event of loss of external communications networks, many utility operations may be compromised, requiring greater reliance on manual operation and assessment of the state of damage. As an example, with the failure of multiple communications systems, it may be difficult to coordinate the activities of repair crews in the field with operational decisions, thus attenuating the hazards for workers and slowing the restoration.



**FIGURE 4.5** Disruption of any material or service that the electricity system relies on can result in loss of electric service and make restoration more challenging.

NOTE: SCADA, supervisory control and data acquisition.

SOURCE: DOE (2017).

### Design for Cyber Resilience

The electric power system has become increasingly reliant on its cyber infrastructure, including computers, communication networks, other control system electronics, smart meters, and other distribution-side cyber assets, in order to achieve its purpose of delivering electricity to the consumer. A compromise of the power grid control system or other portions of the grid cyber infrastructure itself can have serious consequences ranging from a simple disruption of service to permanent damage to hardware that can have long-lasting effects on the performance of the system. Any consideration of improved power grid resilience requires a consideration of improving the resilience of the grid's cyber infrastructure.

Over the past decade, much attention has rightly been placed on grid cybersecurity, but much less has been placed on grid cyber resilience. In particular, there has been significant research and investment in technologies and practices to prevent cyber attacks. Some of the many methods include the following: (1) identifying and apprehending cyber criminals, (2) defending the perimeter of a network with firewalls and

“white listing” and “black listing” certain communications sources, (3) practicing good cyber “hygiene” (e.g., protecting passwords and using two-factor authentication), (4) searching for and removing suspect pernicious code continuously, and (5) designing control systems with safer architecture—for example, segmenting systems to slow or prevent the spread of malware. The sources of guidance on protection as a mechanism to achieve grid cybersecurity are numerous (DOE, 2015); one good source of reference materials specific to industrial control systems can be found at the Department of Homeland Security’s Industrial Control System Cyber Emergency Response Team website.<sup>7</sup> Another good source of information is the Energy Sector Control Systems Working Group’s *Roadmap to Achieve Energy Delivery Systems Cyber Security* (ESCSWG, 2011). Furthermore, strategies to achieve power grid cybersecurity are documented in the National Institute for Standards and Technology Internal/

<sup>7</sup> The website for the Industrial Control System Cyber Emergency Response Team is <https://ics-cert.us-cert.gov/Standards-and-References>, accessed July 4, 2017.



Interagency Report 7628 *Guidelines for Smart Grid Cyber Security* (NISTIR, 2010). A good source of basic information is *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST, 2013), which, although nominally applying to federal information technology systems, has some guidance that can be useful in protecting grid cyber infrastructure.

It is now, however, becoming apparent that protection alone as a mechanism to achieve cybersecurity is insufficient and can never be made perfect. Cyber criminals are difficult to apprehend, and there are nearly 81,000 vulnerabilities in the National Institute of Standards and Technology (NIST) National Vulnerability Database, making it challenging to use safe code (NVD, 2016). An experiment conducted by the National Rural Electric Cooperative Association and N-Dimension in April 2014 determined that a typical small utility is probed or attacked every 3 seconds around the clock. Given the relentless attacks and the challenges of prevention, successful cyber penetrations are inevitable, and there is evidence of increases in the rate of penetration in the past year, particularly ransomware attacks.

Fortunately, the successful attacks to date have largely been concentrated on utility business systems as opposed to monitoring and control systems (termed operational technology [OT] systems), in part because there are fewer attack surfaces, fewer users with more limited privileges, greater use of encryption, and more use of analog technology. However, there is a substantial and growing risk of a successful breach of OT systems, and the potential impacts of such a breach could be significant. Serious risks are posed by further integration of OT systems with utility business systems, despite the potential for significant value and increased efficiency. Furthermore, the lure of the power of Internet protocols and cloud-based services threatens some of the practices that have historically protected the grid. Cloud-based services provide the potential for better reliability, resilience, and security versus on-premises computing, particularly for smaller utilities. For example, major commercial clouds, like the Amazon cloud, have a very high level of around-the-clock monitoring by a well-provisioned security operations center, better than that operated by some utilities. The cloud does, however, present another attack surface. Utilities that choose to use the cloud must explicitly consider the security of the cloud and how to secure the communications bi-directionally.

Given that protection cannot be made perfect, and the risk is growing, cyber resilience, in addition to more classical cyber protection approaches, is critically important. Cyber resilience aims to protect, using established cybersecurity techniques, the best one can but acknowledges that that protection can never be perfect and requires monitoring, detection, and response to provide continuous delivery of electrical service. While some work done under the cybersecurity nomenclature can support cyber resilience (e.g., intrusion detection and response), the majority of the work to date has been focused on preventing the occurrence of

successful attacks, rather than detecting and responding to partially successful attacks that occur.

Cyber resilience has a strong operational component (mechanisms must be provided to monitor, detect, and respond to attacks that occur), but it also has important design-time considerations. In particular, architectures that are resilient to cyber attacks are needed to support cyber resilience. Work during the past decade has resulted in “cybersecurity architectures” for the power grid cyber infrastructure, such as those described by NIST (2015), but there has been much less work done to define “cyber resilience architectures.” Some preliminary discussion of such an architecture can be found in MITRE’s *Cyber Resiliency Engineering Framework* (Bodeau and Graubart, 2011) and in NIST’s *Guidelines for Smart Grid Cyber Security* (NISTIR, 2010), among other places.

Generally speaking, a cyber resilience architecture should implement a strategy for tolerating cyber attacks and other impairments by monitoring the system and dynamically responding to perceived impairments to achieve resilience goals. The resilience goals for the cyber infrastructure require a clear understanding of the interaction between the cyber and physical portions of the power grid as well as how impairments on either (cyber or physical) side could impact the other side. By their nature, such goals are inherently system-specific but should balance the desire to minimize the amount of time a system is compromised and maximize the services provided by the system. Often, instead of taking the system off-line once an attack is detected, a cyber resilience architecture attempts to heal the system while providing critical cyber and physical services. Based on the resilience goals, cyber resilience architectures typically employ sensors to monitor the state of the system on all levels of abstraction. The data from multiple levels are then fused to create higher-level views of the system. Those views aid in detecting attacks and other cyber and physical impairments, as well as in identifying failure to deliver critical services. A response engine, often with human input, determines the best course of action. The goal, after perhaps multiple responses, is complete recovery (i.e., restoring the cyber system to a fully operational state).

Further work to define such cyber resilience architectures that protect, detect, respond, and recover from cyber attacks that occur is critically needed. Equally important, but just as challenging, is work to validate that proposed cyber resilience architectures achieve cyber resilience and cybersecurity requirements (see Recommendation 4.10).

### Regulatory and Institutional Opportunities

As described in Chapter 2, utilities seek and regularly receive regulatory approval for routine preventative maintenance activities such as vegetation management and hardening investments. While FERC regulates generation and interstate transmission, individual states are responsible

**BOX 4.3****Select Regulatory Actions Supporting Hardening, Modernization, and Other Preventative Investments****Florida Storm Hardening**

Given the recurring high risk of hurricane damage to electricity infrastructure in Florida, state regulators have long considered how to improve reliability and resilience to large storms. In a series of rulemakings in the mid-2000s, the Public Service Commission required that investor-owned utilities provide annual hurricane preparedness briefings, file and update storm hardening plans, increase coordination with local governments, and invest in research with Florida universities to improve robustness and recovery.

**Energy Strong New Jersey**

Following Superstorm Sandy and the extensive damage done to regional distribution systems and substations, the New Jersey Board of Public Utilities approved more than \$1 billion for hardening and modernizing Public Service Enterprise Group (PSEG) electric and gas infrastructure. Approximately \$600 million of this will go to elevating 29 substations damaged during Sandy to 1–2 feet above Federal Emergency Management Agency flood levels. An additional \$125 million will be used to install more sectionalizing switches in the distribution network, allowing PSEG to reconfigure the distribution systems and maintain service to the maximum number of customers during outage events.

**Connecticut Act Enhancing Emergency Preparedness and Response**

Passed following Hurricane Irene and major winter storms in 2011, this Act requires utilities to file emergency preparedness plans every 2 years with the state regulatory commission. Additionally, the Act provided grant funding for construction of microgrid projects at critical facilities around the state, and to date more than \$30 million has been invested in nearly 20 projects.

**Illinois Energy Infrastructure Modernization Act**

Passed by the state legislature in 2012, the Act authorizes Commonwealth Edison and Ameren Illinois to invest \$2.6 billion and \$625 million, respectively, in hardening, undergrounding, distribution automation, AML installations, and substation upgrades. The Act sets performance-based rates of return for utilities.

for approving investments in local transmission and the distribution system. There is wide variety in public utility commission (PUC) approval of utility investment across the United States and between geographically similar Gulf states (Carey, 2014). States along the hurricane-prone southeastern coast are more likely to allow alternative mechanisms to finance such investments, including the addition of “riders” to customer bills, securitization and issuance of bonds, and creation of reserve accounts that utilities can use as a form of self-insurance (EEI, 2014).

In addition to approving investments in hardening and preventative strategies, several states, such as California, Florida, and Connecticut, require utilities to regularly submit and update emergency preparedness plans, which often require input and coordination from city and county officials. Others provide performance-based incentives or penalties—for example, based on improvements to reliability measures such as SAIDI and SAIFI (although most reporting standards do not include large-area, long-duration outages when calculating these metrics)—to encourage best practices in the absence of standards on distribution systems. Other states impose penalties for inadequate levels of service or performance during storm events and recovery. Funding of grid modernization investments likewise varies across

states, with some regulator commissions such as California and Massachusetts researching and investing significantly in advanced communications and automation technologies. In the absence of regulatory approval, there is a critical opportunity for continuing federal grants (e.g., the Smart Grid Investment Grant provided to Chattanooga Electric Power Board) to further demonstrate the viability of such technologies and promote wider adoption across states.

In response to large outages such as those that resulted from Superstorm Sandy and other high-profile storms, state PUCs and, to a lesser extent, state legislatures across the country have considered investments in system hardening and implementing assorted grid modernization strategies with the goal of preventing or mitigating the impact of future large outages (Box 4.3).<sup>8</sup> Historically, such crises often provide the opportunity to focus attention and resources on costly robustness and resilience enhancements in a system that may be optimized economically without systematic consideration of the value of avoiding or responding quickly to these extreme events. Nonetheless, regulators’ and the industry’s efforts are more often reactive than proactive,

<sup>8</sup> A more complete review of state regulatory actions related to robustness and resilience is provided by EEI (2014).



and a focus on near-term cost-benefit optimization may not have resulted in investments that provide cost-effective benefits from a more resilient power grid. Thus, the committee expects that successfully funding cost-effective investments in resilience will require novel approaches, as described in Chapter 7, and proper metrics, as described in Recommendation 2.1.

## OPERATIONS

Much can be done in the area of real-time electric grid operations to enhance physical and cyber resilience. With the advent of smart grid devices, the electric grid is getting more intelligent with more sensing and embedded controls. While they are certainly beneficial, smart grid devices make the grid more complex. While this automatic control is helpful, any consideration of power system operations needs to recognize that the human operators are still very much “in the loop” and will continue to be so for many years into the future. Therefore, strategies to enhance operational resilience need to include tools to enhance the capabilities of the operators and engineers running the system.

In order to understand operations, it is useful to consider the different power system operating states shown in Figure 4.6. By far the majority of the time is spent in the normal state—that is, ready to handle the N-1 reliability criteria. This is the state in which people have the most experience; hence, many of the tools used in the control center are focused on normal operations. More rarely, the system moves into alert, emergency, and restorative situations. However, such situations are encountered often enough that there is good historical experience; control room personnel train for such situations, and, for the most part, they have adequate tools for dealing with these situations.

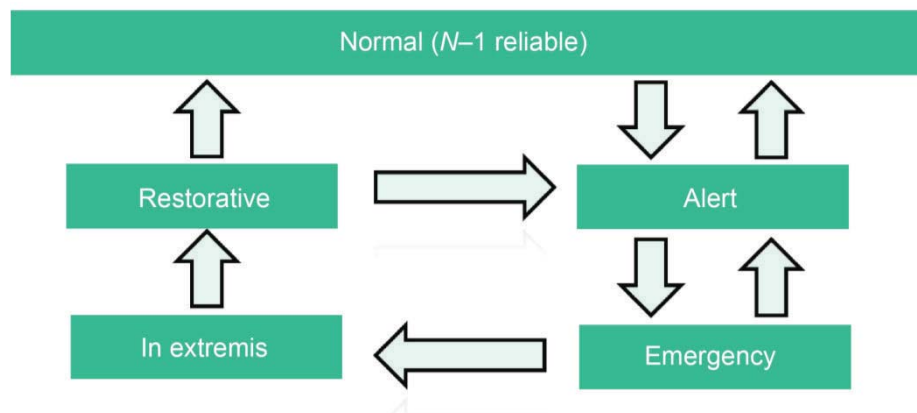
Enhancing grid resilience requires that more attention be given to the alert, emergency, in extremis, and restorative

stages of these operating states. In these stages, the previously interconnected grid may be broken into a number of electrical islands, and the operation of these islands may need to be performed by entities that are not normally responsible for grid operations (NERC, 2012a).

Sometimes, threats such as hurricanes can be identified with sufficient warning time to allow system operators to preemptively position the system to be more robust and able to respond to emerging conditions. This often involves curtailing any avoidable outages that might be caused by maintenance or other activities, deploying additional reserves to the extent possible, and even powering down certain critical components to minimize potential damage. This strategy is often less expensive than hardening strategies previously discussed. All major events are managed by operators in the control center, and their skills and training, as well as their tools and supporting technologies, are critical factors for how effectively the event will be managed.

## Wide-Area Monitoring and Control

As the power grid becomes more complex and is operated closer to reliability limits, the need for greater remote control increases. Fortunately, the technologies needed for such “wide-area control,” principally sensors and communications, are becoming cheaper and more powerful. The increasing use of high-speed wide-area measurements, including synchrophasors that measure currents and voltages 30–60 times a second and communicate them to distant computers, allows the design of controls that can use input data from different parts of the system and send control signals to equipment in different locations. The combination of PMUs, distribution automation, dedicated fiber-optic cable communications infrastructure, and affordable computing will likely lead to increasing reliance on artificial intelligence



**FIGURE 4.6** Power system operating states.

SOURCE: © 1978 IEEE. Reprinted, with permission, from *IEEE Spectrum Operating under Stress and Strain [electrical power systems control under emergency conditions]*.

in the power system. Additionally, remedial action schemes<sup>9</sup> are increasingly being deployed to increase the throughput of the grid, while minimizing the risk of cascading failures, by appropriately tripping loads and generators after an event on the system. The measurements for these automatic relays can often be hundreds of miles apart. These automated systems are able to sense and take action in real time, and can be thought of as a stepping stone to wider application of artificial intelligence and machine learning applied to the power grid.

Although such wide-area controls are appearing all over the world, the design, simulation, on-line testing, and cyber protection of such controls are expensive and time-consuming. Moreover, the architecture of the power grid and its overlaid control system has a direct impact on the design of such controls. For example, how centralized or decentralized a control scheme should be is constrained by where the measurements are, the communication paths to gather these measurements in the controller, and which equipment are available to this controller for control. Such controllers are in their evolutionary stages, so they should be designed not just for economic and reliability benefits, but also for resilience.

Often the term smart grid is used in reference to electronic meters and sensors. However, it also encompasses the wide-area monitoring and control considered here. That is, smart grids could include automatic sectionalizing, smart islanding to prevent cascading failures, the ability to operate these islands in a degraded state, and supercomputing resources to support system operators. For example, during the August 14, 2003, blackout, there was almost an hour of opportunity to intervene before the cascading event initiated (USCPSOTF, 2004). With better operational intelligence, a preventative shedding of approximately 2,000 MW load in the Cleveland area would have prevented the cascading failure that affected more than 60 million people.

During a major event such as Hurricane Katrina or Superstorm Sandy, thousands of alarms can overwhelm the system operator. Artificial intelligence could help quickly prioritize these alarms that come in over the supervisory control and data acquisition (SCADA)/energy management systems (EMS) and provide the operator with suggestions for the most important alarms to focus on, the root cause(s) of the event, and the most important actions to prevent further degradation and start restoration. The inherent complexity that power system operators have to face every day used to be addressed through detailed procedures. Today, with the system growing in complexity, the assistance of artificial intelligence and improved man-machine interfaces for system operators is likely to enhance both reliability and resilience. Under this scenario, all historical events and previous operators' experiences could be accumulated by a

system such as IBM's Watson to prioritize alarms and suggest appropriate action.

As DERs and smart inverters become more and more common in the distribution system, electricity system operators need to assess whether artificial intelligence combined with closed-loop fiber-optic broadband communication can improve the reliability and resilience for distribution customers. As more DERs are connected with smart inverters, the distribution system can break into smaller microgrids that can island and maintain service to critical load. In addition to distributed generation, demand side resources (customer loads) with inverters and power electronics can improve both reliability and resilience.

The Chattanooga EPB has demonstrated this by installing fiber-optic communication and automatic sectionalizing switches. Its communication system brought fiber optics to every home with smart meters available to determine both billing information and operational data such as Volts, Volt-ampere reactives, and Amps. This alone will not improve resilience, but combined with automated switches and voltage control devices EPB has greatly improved both the reliability and the resilience of its distribution system.

**Finding:** New automation systems promise to enable better monitoring and control of the grid. The design of such large-scale, wide-area controllers should be done with cyber resilience in mind. Such controllers should tolerate accidental failures and malicious attacks that occur, providing degraded functionality even during recovery from such attacks, and not be a hindrance during catastrophic events or the recovery afterwards. Flexibility of the controller may be achieved with the proper centralized/decentralized design, where the centralized control may provide the best benefits during normal operation. When the grid is broken up after a catastrophic event, however, the decentralized portion may still be able to operate the various parts.

### Physical and Cyber Situation Awareness

Bulk electric grids are some of the world's largest and most complex machines, and disturbances (cyber or physical) can rapidly propagate through their systems. Hence, normal operations can quickly change, demanding quick responses by the human operators or preprogrammed automation. Resilient operation requires physical and cyber "situation awareness," defined as "the perception of critical elements in the environment, the comprehension of their meaning, and the projection of their status into the future" (Wickens et al., 2013), so that unfavorable changes of physical or cyber state that occur can be addressed (either by human or automated means) quickly enough to prevent a catastrophic event.

In the power industry, the term "situation awareness" was popularized by the August 14, 2003, *Blackout Final Report* in which "inadequate situational awareness at First Energy"

<sup>9</sup> A scheme designed to detect predetermined system conditions and automatically take corrective actions that may include, but are not limited to, adjusting or tripping generation, tripping load, or reconfiguring a system (NERC, 2014c).

was noted as the second of the four root causes of the event (USCPSOTF, 2004). The importance of system understanding was also highlighted in the first and fourth causes of the event: “FirstEnergy (FE) and ECAR (East Central Area Reliability Council) failed to assess and understand the inadequacies of First Energy’s system, particularly with respect to voltage instability and the vulnerability of the Cleveland-Akron area, and FE did not operate its system with appropriate voltage criteria. . . . [T]he interconnected grid’s reliability organizations [failed] to provide effective real-time diagnostic support” (USCPSOTF, 2004). If operators were aware of the accurate estimate of the “true state” of the grid, they could have taken appropriate actions, which would have eliminated the propagation of effects that led to the widespread blackout. Thus real-time determination of the combined physical and cyber state of the grid is needed to achieve resilience.

Whether operator action can prevent a blackout depends on the time frame and severity of the event (Overbye and Weber, 2015). Some large-scale blackouts cannot be prevented by operator action; earthquakes are examples of unanticipated events that can cause severe damage within seconds. Cyber attacks also have the potential to spread extremely quickly. Conversely, slow-moving weather systems such as hurricanes or ice storms give operators plenty of time to act, but the blackouts cannot be fully prevented. As an example, an ice storm in January 1998 resulted in the collapse of more than 770 transmission towers, causing a large-scale blackout in Canada (Hauer and Dagle, 1999), and Superstorm Sandy caused 8.5 million customer power outages in 2012 (Abi-Samra et al., 2014). The same might be true of the pandemics that would severely limit human resources for response (NERC, 2010).

However, many potential blackouts, including a number of the severe events considered here, do have time frames that could allow for effective operator intervention. North American examples include the August 14, 2003, blackout that affected more than 50 million people, in which more than an hour passed between the system being outside of the normal secure state (remaining stable following the next contingency) and the final uncontrolled cascading failure leading to the blackout (USCPSOTF, 2004); and the September 8, 2011, Western Electricity Coordinating Council blackout that had an 11-minute period between the initiating event and the blackout, and that cited lack of situation awareness as a cause (FERC and NERC, 2012). A primary reason for these time frames is the underlying power system dynamics, including the time constants associated with thermal heating on transmission lines and transformers, the operation of load-tap-changing transformers, protective relaying time constants, and other system limits. Another reason would be the dynamics associated with the initiating event; for a GMD, this might be minutes to hours. Having good power system situation awareness, even during periods of extremely unusual system stress, is crucial for enhancing overall grid resilience.

Furthermore, propagation of disturbances through the grid can potentially be mitigated before a catastrophic event occurs though the use of cyber-resilient, computer-enabled, automated monitoring and state estimation, diagnosis, response, and recovery. While humans can only react on time scales that are in seconds-to-minutes, computer-enabled diagnosis, response, and recovery can operate on the time scale of microseconds-to-seconds, effectively halting the propagation of adverse effects before they progress to a stage where they can no longer be mitigated. Hence the development of (1) deep and diverse monitoring mechanisms, (2) computerized monitor data fusion methods, and (3) computerized response selection and actuation methods that themselves are cyber resilient is essential to providing resilience in the face of a wide variety of impairments.

### Cyber-Resilient Monitoring of Physical and Cyber States

Regarding monitoring, methods must be developed to determine the amount and diversity of monitoring necessary to gain the cyber and physical situation awareness to effectively respond to particular classes of impairments. Today, monitor selection and deployment is typically a static and off-line process. Methods are also needed to increase the confidence in the monitoring data that are obtained. It is critical that the state estimated from the monitoring data used by a resilience strategy is not influenced by bad data (created either inadvertently or through deliberate attacker action) so as to avoid response decisions that compromise resilience.

### Monitor Data Fusion

A key challenge with the effective use of monitor data (whether cyber or physical) is their volume. In order to make sense of this large volume of monitor data, methods are needed to fuse the data into higher level knowledge about the state of the grid, creating actionable situation awareness. Fusion, in this context, is defined as the process to combine information from multiple sources to achieve inferences, which will be more efficient and more accurate than if they were achieved through a single source. A key challenge in the power grid context is that monitoring data concerning both the physical and cyber state of the grid is needed and must be fused together to understand the state of the system to the degree that response actions to preserve correct operation can be taken.

Understanding of the system is complicated by the fact that when a monitor signals a problem, it is unclear whether the problem is with the component or sub-system that is being monitored or with the monitor itself (particularly if malicious actions might cause erroneous monitor data). Monitoring of the state of both cyber and physical aspects of the grid is essential and must be sufficiently powerful to diagnose whether the error-condition being observed is due to a cyber and/or physical impairment. While it has been long



understood that the monitoring of physical aspects of the grid is needed, the criticality of the monitoring of the state of the grid's cyber components is less understood.

Human operators will continue to play a key role in grid operations for decades to come, and they can certainly help in the fusion of information. Important goals include minimizing the overhead on human experts and learning from the monitor data to identify important features that can contribute to lack of resilience. It would also be valuable if these techniques are computationally lightweight. This would allow operators to incorporate these techniques in the system to work online.

### Response Selection and Actuation

Timely response to detection of undesirable state conditions is critical to maintain the grid's ability to deliver power despite impairments that occur. In order to be effective, determination of response actions must be efficient and scalable. In particular, a resilience response mechanism must respond quickly in a way that limits the cyber or

physical impairment (whether accidental or intentional) from propagating to the point that a catastrophic event occurs. Furthermore, resilience response mechanisms must be scalable, in order to account for the unique physical and cyber complexity of the grid and the large volume of monitor data that must be collected, to obtain an accurate estimate of the state of the system.

During the unusual situations associated with severe events, wide-area power system visualization is crucial for providing the operators and engineers with the "big picture" of a grid that may be operating in a physical and/or cyber state they have not previously encountered. There may be multiple electric islands, transmission line flows may be substantially different from normal, and the voltage profile could be quite unusual. Often this wide-area view is provided in a control center using a mapboard, such as the one used by Independent System Operator (ISO) New England's control center, shown in Figure 4.7. As noted by Overbye and Weber (2015), such wide-area visualizations are divided into two main types. The first approach is to draw the display using fairly precise geographic coordinates. An example of this



**FIGURE 4.7** ISO New England control room.  
SOURCE: ISONE (2013).

is shown for the synthetic network in Figure 4.4 or in the coupling with the earthquake simulations by Veeramany et al. (2016). Advantages include the ability to overlay power system information with other infrastructures and a familiar context when communicating with non-power engineers. A key disadvantage is that often the locations with a large amount of electrical infrastructure, such as urban areas, have a small geographic footprint. An alternative approach is to use a pseudo-geographic layout in which the position of the power system elements has some relationship with their actual geographic coordinates, but the display is arranged for electrical clarity. This approach was used in the ISO New England control center, which, while covering all of New England, has much of the display devoted to the greater Boston area. Additional visualization techniques, such as color contouring, focus on displaying large amounts of power system information (Weber and Overbye, 2000).

There is also a need to consider the human factors of severe events in the control room context. During such events, there would certainly be a high level of stress, and, while expert operators would be better prepared than less experienced personnel, successful decisions are far from guaranteed. Wickens et al. (2013) explain, “Cues may be uncorrelated, overconfidence may shortchange cognitive monitoring, and rapid pattern-recognition classification may overlook a single outlying cause.” There may also be a “confirmation bias,” which “describes a tendency for people to seek information and cues that confirm the tentatively held hypothesis or seek (or discount) those that support an opposite conclusion or belief” (Wickens et al., 2013). This reinforces the importance of training and drills that provide operators with simulated experience.

**Finding:** Bulk electric grids are not only some of the world's largest and most complex machines, but they also have been architected in a way that disturbances can, if not mitigated, rapidly propagate through the system. Maintaining physical and cyber situation awareness at all times is key. Lack of situation awareness has been a contributing factor in a number of recent large-scale outages. During severe events, this will be even more of a challenge; therefore, there is a need for work on the development of data analytics and visualization techniques that will allow operators and engineers to maintain cyber and physical situation awareness.

**Recommendation 4.8:** The Department of Energy and the National Science Foundation should fund research on enhanced power system wide-area monitoring and control and on the application of artificial intelligence to the power system. Such work should include how the human–computer interface and visualization could improve reliability and resilience. In particular, the Department of Energy should develop research programs on enhancing power grid control room cyber and physical situation awareness with a focus on severe event situations.

### Monitoring of Grid Cyber System State to Achieve Physical and Cyber Resilience

The proper functioning of the grid's various cyber systems (e.g., computers, communications) directly affects the ability to monitor, operate, and control the power system, thus making it imperative that the cyber system itself also be resilient. Like the physical aspects of the power grid, these cyber systems can be affected by catastrophic events like storms and earthquakes and are directly vulnerable to cyber attacks. These supporting systems are often considered critical and are usually designed with enough redundancy to provide reliability to accidental faults. It is critical to have situation awareness of the state of information systems alongside operations systems, as detailed in the concept of an integrated security operations center (EPRI, 2013).

While existing NERC standards provide some requirements with respect to cybersecurity, no standards or widespread best practices exist for tolerating deliberate cyber attacks. Moreover, monitoring of the system itself has been less stringent than that of the power system, and, unlike the power system, the status of the control system is rarely shared with that of the neighboring power companies. For example, during the 2003 Northeast blackout the neighboring power companies were not aware that several of the monitoring functions like alarm processing and state estimation were not functioning at the Akron, Ohio, control center.

Even less common is the use of architectural approaches to ensure the resilience of the cyber system to accidental failures and malicious attacks. As noted, the operation of an interconnected power grid requires the cooperation of many entities, mostly done through the coordination among dozens of control centers. Thus, the health of the control and communications systems should also be continuously monitored by these control centers. These monitoring data should be used to take actions to maintain the resilience of the cyber system itself to both accidental failures and malicious attacks and be shared with all the others who depend on this coordination.

Unfortunately, data gathering and analysis are often performed separately and differently between neighboring utilities and between T&D sections within the same power company. More coordination between these jurisdictions would be helpful during normal operations; the lack of it severely affects the ability to prevent large-scale catastrophes like a cascading failure or cyber attack. During such an event that impacts several power companies, effective communication of data among utilities can help inform and accelerate decisions that may avoid permanent damage to existing hardware or prevent widespread outages. The main issue in coordinating these various functions has been the lack of standardization of data definitions, databases, and communication protocols. Moreover, data exchange between neighbors also raises some proprietary issues. However, if resilience is to be increased and the ability to recover from catastrophic events is to be accelerated, such coordination between T&D in the same

company and between interconnected neighboring companies is necessary. Although the utility industry has a long record of collaboration during large-scale disturbances, this is still done more on an ad hoc basis; the type of coordination suggested here must be planned, and the tools must be in place long before the catastrophe.

Achieving greater standardization is important and an active research area in Europe, providing opportunities for strong coordination (EDSO, 2015). However, as that occurs, it is important to devote serious attention to cybersecurity lest identical control equipment, with identical vulnerabilities, be used by multiple companies. This could make the system particularly vulnerable to a cyber attack that could be widespread and affect multiple utilities simultaneously.

**Finding:** The cyber system that monitors, analyzes, and controls the physical components of the power grid is critical to providing efficient and reliable service from the grid. Less attention has been placed on making these cyber systems resilient. Furthermore, the various control systems of an interconnected power grid fall under many different jurisdictions, and close coordination is needed for the design and operation so that information exchange in real time is seamless and timely and response actions are taken in a coordinated way.

**Finding:** Currently, there is a lack of standardized information sharing among utilities at the T&D levels. In some cases, such as cyber health data, the data requirements have not yet been defined. As greater standardization is achieved, greater attention must also be given to cybersecurity and risks of common-mode failures.

**Recommendation 4.9:** The Department of Energy should lead and coordinate an effort among the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation, the National Association of Regulatory Utility Commissioners, and the states to develop standardized data definitions, communication protocols, and industrial control system designs for the sharing of both physical and cyber system health information. The goal of standardizing data definitions and communication protocols would be to improve the awareness of the operating conditions of all interconnected power systems for all involved transmission operators and distribution operators.

### Architectures for Providing Cyber and Physical Resilience

A wide range of cyber systems are used to protect and control the grid. In operations, the time requirements for response to maintain resilience range from a few milliseconds (e.g., for protective relays controlling circuit breakers that clear faults), to seconds (e.g., for the automatic generation control that provides real-time dispatch to generators), to several seconds to minutes (e.g., for the software used by

the operators for human-in-the-loop control). Much of this architecture, and its enhancement via synchrophasors, is discussed by Bose (2010).

Transmission operators use EMS to monitor and control the grid. Almost all of the real-time measurements input to the EMS come from SCADA systems, which scan the grid every 2 to 4 seconds. An important component of EMS is the monitoring/alarming system that notifies the operator when unusual situations are encountered. This alarm system failed for one transmission operator leading up to the August 14, 2003, blackout, which contributed to its lack of situation awareness (USCPSOTF, 2004). As the name implies, SCADA is used for direct monitoring and control of the grid. A failure of SCADA, such as from a cyber intrusion, would make operations very difficult, requiring personnel to be physically located at key electric substations. Over the past several years, the SCADA data are increasingly being supplemented by PMU data, which uses much faster scan rates of 30 to 60 times per second, allowing direct measurement of the voltage and current phase angles (NASPI, 2015).

In order to run more advanced grid analysis techniques in real time, the imperfect measurements from SCADA (and sometimes PMUs) are input to a process known as state estimation. State estimation is run every few minutes to obtain a best estimate of power system voltages and currents. The output of the state estimator is then fed to applications such as power flow, contingency analysis, security-constrained optimal power flow, and transient stability analysis. State estimation is a maximum likelihood estimator that uses iterative algorithms. In a modern control center, the state estimator might be solving on the order of 250,000 measurements every minute, with convergence rates well over 98 percent of the time (PJM, 2016). However, during unusual situations associated with severe events, convergence of the state estimator itself might be an issue. This was the case during the August 14, 2003, blackout, in which lack of convergence in the Midwest Independent Transmission System Operator state estimator contributed to its inability to provide real-time diagnostic support (USCPSOTF, 2004).

The grid was operated for more than half a century before computers were invented and can still be, in many cases, operated in a degraded way without the advantages of the computerized control system. In fact, the cyber attack on the Ukraine system forced the operators to operate the power grid with reduced levels of service without the automation system, which was badly compromised.

**Finding:** The control system for the power grid must be designed and operated in a way that allows it to tolerate both accidental faults and malicious attacks. Best practices from the dependable computing community and the emerging cyber resilience community could be employed and extended to make the grid cyber infrastructure itself resilient. Moreover, the interfaces between the cyber control system and the physical aspects of the power grid could be designed



in such a way that the power grid can be operated without automation, albeit in a degraded mode. This would require some control functions to be performed manually during catastrophic events, thus requiring personnel to be trained and ready to perform functions that would rarely be needed.

**Recommendation 4.10:** The Department of Energy should embark upon a research, development, and demonstration program, utilizing the diverse expertise of industry, academia, and national laboratories, that results in a prototypical cyber-physical-social control system architecture for resilient electric power systems. The program would have the following components: (1) A diverse set of sensors (spanning the physical, cyber, and social domains), (2) a method to fuse this sensor data together to provide situation awareness of known high quality, and (3) an ability to generate real-time command and control recommendations for adaptations that should be taken to maintain the resilience of an electric power system. This should include research to develop methods for specifying anomalous operating conditions, so that anomaly detection systems can be deployed widely to aid in the detection of cyber intrusions. In this process, the Department of Energy should coordinate with standards-setting organizations. Analytic arguments should be constructed so that these recommendations do not compromise the safety or availability of the system.

## REFERENCES

- Abi-Samra, N., J. McConnach, S. Mukhopadhyay, and B. Wojszczyk. 2014. When the bough breaks: Managing extreme weather events affecting electrical power grids. *IEEE Power and Energy Magazine* 12(5): 61–65.
- Albertson, V.D., J.M. Thorson Jr., R.E. Clayton, and S.C. Tripathy. 1973. Solar-induced currents in power systems: Cause and effects. *IEEE Transactions on Power Apparatus and Systems* PAS-92(2): 471–477.
- ARPA-E (Advanced Research Projects Agency-Energy). 2016. “Grid Data.” <https://arpa-e.energy.gov/?q=arpa-e-programs/grid-data>. Accessed July 13, 2017.
- Bedrosian, P.A., and J.J. Love. 2015. Mapping geoelectric fields during magnetic storms: Synthetic analysis of empirical United States impedances. *Geophysical Research Letters* 42(10): 160–170.
- Birchfield, A.B., T. Xu, K. Gegner, K.S. Shetye, and T.J. Overbye. 2016. Grid structural characteristics as validation criteria for synthetic networks. *IEEE Transactions on Power Systems* 32(4): 3258–3265.
- Bodeau, D.J., and R. Graubart. 2011. *Cyber Resiliency Engineering Framework*. MITRE Technical Report 110237. [https://www.mitre.org/sites/default/files/pdf/11\\_4436.pdf](https://www.mitre.org/sites/default/files/pdf/11_4436.pdf).
- Bose, A. 2010. Smart transmission grid applications and their supporting infrastructure. *IEEE Transactions on Smart Grid* 1(1): 11–19.
- Boteler, D. 1994. Geomagnetically induced currents: Present knowledge and future research. *IEEE Transactions on Power Delivery* 9(1): 50–58.
- Carey, K. 2014. *The Day After Tomorrow: A Survey of How Gulf Coast State Utility Commissions and Utilities are Preparing for Future Storms*. <http://wordpress.ei.columbia.edu/climate-change-law/files/2016/06/Carey-2014-03-Gulf-Coast-State-Utility-Commissions-Storm-Preparation.pdf>.
- CEC (California Energy Commission). 2016. *Aliso Canyon Action Plan to Preserve Gas and Electric Reliability for the Los Angeles Basin*. [http://www.energy.ca.gov/2016\\_energypolicy/documents/2016-04-08\\_joint\\_agency\\_workshop/Aliso\\_Canyon\\_Action\\_Plan\\_to\\_Preserve\\_Gas\\_and\\_Electric\\_Reliability\\_for\\_the\\_Los\\_Angeles\\_Basin.pdf](http://www.energy.ca.gov/2016_energypolicy/documents/2016-04-08_joint_agency_workshop/Aliso_Canyon_Action_Plan_to_Preserve_Gas_and_Electric_Reliability_for_the_Los_Angeles_Basin.pdf).
- DOE (Department of Energy). 2011. *A Smarter Electric Circuit: Electric Power Board of Chattanooga Makes the Switch*. [https://www.smartgrid.gov/files/EPB\\_Profile\\_casestudy.pdf](https://www.smartgrid.gov/files/EPB_Profile_casestudy.pdf).
- DOE. 2015. *Energy Sector Cybersecurity Framework Implementation Guidance*. [https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance\\_FINAL\\_01-05-15.pdf](https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf).
- DOE. 2017. *Quadrennial Energy Review: Transforming the Nation's Electricity System: The Second Installment of the QER*. <https://energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review-Second%20Installment%20%28Full%20Report%29.pdf>.
- EDSO (European Distribution System Operators for Smart Grids). 2015. *Coordination of Transmission and Distribution System Operators: A Key Step of the Energy Union*. <http://www.edsoforsmartgrids.eu/wp-content/uploads/public/Coordination-of-transmission-and-distribution-system-operators-May-2015.pdf>.
- EEL (Edison Electric Institute). 2014. *Before and After the Storm*. <http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/BeforeandAftertheStorm.pdf>.
- EPRI (Electric Power Research Institute). 2013. *Guidelines for Planning an Integrated Security Operations Center*. EPRI Report # 3002000374. Palo Alto, Calif.: EPRI.
- ESCSWG (Energy Sector Control Systems Working Group). 2011. *Roadmap to Achieve Energy Delivery Systems Cyber Security*. [https://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap\\_finalweb.pdf](https://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf).
- FERC (Federal Energy Regulatory Commission) and NERC (North American Electric Reliability Corporation). 2012. *Arizona-Southern California Outages on September 8, 2011: Causes and Recommendations*. <https://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf>.
- Glass, J. 2016. “Enhancing the Resiliency of the Nation’s Electric Power Transmission and Distribution System,” presentation to the Committee on Enhancing the Resilience of the Nation’s Electric Power Transmission and Distribution System, September 29, Washington, D.C.
- Hart, D., and A. Sarkissian. 2016. *Deployment of Grid-Scale Batteries in the United States*. <https://energy.gov/sites/prod/files/2017/01/f34/Deployment%20of%20Grid-Scale%20Batteries%20in%20the%20United%20States.pdf>.
- Hauer, J.F., and J.E. Dagle. 1999. *Consortium for Electric Reliability Technology Solutions: Grid of the Future*. PNNL-13150. Richland: Pacific Northwest National Laboratory.
- Hutchins, T., and T.J. Overbye. 2016. Power system dynamic performance during the late-time (E3) high-altitude electromagnetic pulse. *Proceedings of the 19th Power Systems Computation Conference*. Genoa, Italy, June 20–24.
- ICF. 2016. *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. <https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf>.
- IEEE (Institute of Electrical and Electronics Engineers). 2017. “Project P1547—Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces.” <https://standards.ieee.org/develop/project/1547.html>. Accessed March 2017.
- ISONE (Independent System Operator New England). 2013. ISO New England Control Room. <https://www.linkedin.com/company/iso-new-england>. Accessed July 11, 2017.
- Lordan, R. 2016. “Transmission Resiliency & Security Response to High Impact Low Frequency Threats,” presentation at the NCSL-NARUC Energy Risk & Critical Infrastructure Protection Workshop, May 25, Denver, Colo.

## STRATEGIES TO PREPARE FOR AND MITIGATE LARGE-AREA, LONG-DURATION BLACKOUTS

- NASEM (National Academies of Sciences, Engineering, and Medicine). 2016a. *Electricity Use in Rural and Islanded Communities: Proceedings of a Workshop*. Washington, D.C.: The National Academies Press.
- NASEM. 2016b. *Analytic Research Foundations for the Next-Generation Electric Grid*. Washington, D.C.: The National Academies Press.
- NASPI (North American Synchrophasor Initiative). 2015. *NASPI 2014 Survey of Synchrophasor System Networks—Results and Findings*. <https://www.naspi.org/documents>. Accessed July 11, 2017.
- NERC (North American Electric Reliability Corporation). 2005. *TLP-001-4—Transmission System Planning Performance Requirements*. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-001-4&title=Transmission%20System%20Planning%20Performance%20Requirements&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-001-4&title=Transmission%20System%20Planning%20Performance%20Requirements&jurisdiction=United%20States). Accessed January 12, 2017.
- NERC. 2010. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*. <http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf>.
- NERC. 2011. *Report on Outages and Curtailments During the Southwest Cold Weather Event of February 1–5, 2011*. [http://www.nerc.com/files/sw\\_cold\\_weather\\_event\\_final\\_report.pdf](http://www.nerc.com/files/sw_cold_weather_event_final_report.pdf).
- NERC. 2012a. *Severe Impact Resilience: Considerations and Recommendations*. [http://www.nerc.com/docs/oc/sirtf/SIRTf\\_Final\\_May\\_9\\_2012-Board\\_Accepted.pdf](http://www.nerc.com/docs/oc/sirtf/SIRTf_Final_May_9_2012-Board_Accepted.pdf).
- NERC. 2012b. *Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System*. <http://www.nerc.com/files/2012GMD.pdf>.
- NERC. 2013. *Protection System Response to Power Swings*. [http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report\\_Final\\_20131015.pdf](http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf).
- NERC. 2014a. *Standard CIP-014-2*. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=PhysicalSecurity&jurisdiction=null](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=PhysicalSecurity&jurisdiction=null). Accessed January 12, 2017.
- NERC. 2014b. *Polar Vortex Review*. [http://www.nerc.com/pa/trm/January%202014%20Polar%20Vortex%20Review/Polar\\_Vortex\\_Review\\_29\\_Sept\\_2014\\_Final.pdf](http://www.nerc.com/pa/trm/January%202014%20Polar%20Vortex%20Review/Polar_Vortex_Review_29_Sept_2014_Final.pdf).
- NERC. 2014c. *Remedial Action Scheme: Definition Development*. [http://www.nerc.com/pa/Stand/Prjct201005\\_2SpclPrctnSstmPhs2/FAQ\\_RAS\\_Definition\\_0604\\_final.pdf](http://www.nerc.com/pa/Stand/Prjct201005_2SpclPrctnSstmPhs2/FAQ_RAS_Definition_0604_final.pdf).
- NERC. 2015. *PRC-006-2—Automatic Underfrequency Load Shedding*. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-006-2&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-2&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States). Accessed January 12, 2017.
- NERC. 2016a. *TPL-007-1—Transmission System Planned Performance for Geomagnetic Disturbance Events*. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States). Accessed July 3, 2017.
- NERC. 2016b. *Short-term Special Assessment*. [http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20GAS%20Electric\\_Final.pdf](http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20GAS%20Electric_Final.pdf).
- NIST (National Institute of Standards and Technology). 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication 800-53. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
- NIST. 2015. *Guide to Industrial Control Systems (ICS) Cybersecurity*. NIST Special Publication 800-82. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>.
- NISTIR (National Institute of Standards and Technology Internal/Interagency Reports). 2010. *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*. [https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628\\_total.pdf](https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf).
- NREL (National Renewable Energy Laboratory). 2014. *Issue Brief: A Survey of State Policies to Support Utility-Scale and Distributed Energy Storage*. <http://www.nrel.gov/docs/fy14osti/62726.pdf>.
- NVD (National Vulnerability Database). 2016. National Vulnerability Database (NVD)—NVD Dashboard. <https://nvd.nist.gov/general/nvd-dashboard>. Accessed July 11, 2017.
- Overbye, T.J., and J.D. Weber. 2015. Smart grid wide-area transmission system visualization. *Engineering* 1(4): 466–474.
- Overbye, T.J., T.R. Hutchins, K. Shetye, J. Weber, and S. Dahman. 2012. Integration of geomagnetic disturbance modeling into the power flow: A methodology for large-scale system studies. *Proceedings of the 2012 North American Power Symposium*. Champaign, Ill., September 9–11.
- PJM. 2016. *Operations Support Division, Energy Management System (EMS) Model Updates and Quality Assurance (QA) Manual M-03A (Revision 12)*. <http://www.pjm.com/~media/documents/manuals/m03a.ashx>. Accessed July 11, 2017.
- Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly. 2001. Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 21(6): 11–25.
- Rivera, M., and M. Backhaus. 2015. *Review of the GMD Benchmark Event in TPL-007-1*. Los Alamos National Laboratory. [http://www.energy.gov/sites/prod/files/2015/09/f26/TPL-007-1%20Review\\_LANL\\_2015\\_09\\_14.pdf](http://www.energy.gov/sites/prod/files/2015/09/f26/TPL-007-1%20Review_LANL_2015_09_14.pdf).
- USCPSOTF (U.S.–Canada Power System Outage Task Force). 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. <http://www.nerc.com/docs/docs/blackout/ch1-3.pdf>.
- Veeramany, A., G.A. Coles, S.D. Unwin, T.B. Nguyen, and J.E. Dagle. 2016. *Trial Implementation of the High-Impact, Low-Frequency Power Grid Event Risk Framework to Support Informed Decision-Making Placeholder on Earthquakes*. Richland, Wash.: Pacific Northwest National Laboratory.
- Wade, D. 2016. “Increasing the Resiliency/Reliability of the EPB System,” presentation at the Electricity Use in Rural and Islanded Communities: A Workshop Supporting the Quadrennial Energy Review’s Public Outreach, February 8, Washington, D.C.
- Weber, J.D., and T. J. Overbye. 2000. Voltage contours for power system visualization. *IEEE Trans. on Power Systems* 15(1): 404–409.
- Wickens, C.D., J.G. Hollands, S. Banbury, and R. Parasuraman. 2013. *Engineering Psychology and Human Performance*. Fourth Edition. Boston: Pearson.
- Wischkaemper, J.A., C.L. Benner, B.D. Russell, and K.M. Manivannan. 2014. “Waveform Analytics-based Improvements in Situational Awareness, Feeder, Visibility, and Operational Efficiency.” *Proceedings of the 2014 IEEE PES T&D Conference and Exposition*. doi:10.1109/tdc.2014.6863349.
- Wischkaemper, J.A., C.L. Benner, B.D. Russell, and K.M. Manivannan. 2015. Application of waveform analytics for improved situational awareness of electric distribution feeders. *IEEE Transactions on Smart Grid* 6(4): 2041–2049.
- You, H., V. Vittal, and X. Wang. 2004. Slow coherency-based islanding. *IEEE Transactions on Power Systems* 19(1): 483–491.

## 5

## Strategies for Reducing the Harmful Consequences from Loss of Grid Power

### INTRODUCTION

Chapter 4 examined planning, design, and operations that can help improve the reliability and resilience of the grid to prevent or reduce the duration of grid outages. Chapter 6 looks at restoration of grid service. But in the middle sits the question of how to design and plan for a society that will be resilient even with the loss of power. This chapter examines current and future responses to that question. As introduced in Chapter 3, the exact form of that planning depends on the causes of grid failure, because those causes may affect which other services are available and the speed and extent of restoration (see Figure 3.2). Full restoration, as explored in Chapter 6, may take a long time—during and after which the effects of lost grid service could continue to reverberate through society.

As in the other sections of this report, the committee does not focus much on small routine disruptions that are inherent to power distribution systems. Those outages, because they are short and familiar, do not create major resilience problems; their effects are usually local, understood, and well within the range of imagination and planning. Indeed, in a typical year there are about 3,200 significant outages on power grids in the United States, with extreme weather and falling trees as leading causes (Eaton, 2016). In a 2015 Harris poll, homeowners self-reported that one out of four had experienced power outages for 12 hours or longer in the past 2 years (Briggs and Stratton, 2015). These are common events that generate large costs to the economy and public welfare—for example, jeopardizing the continued operation of home health care equipment (Ryan et al., 2015) as well as continuity of important public functions and economic activity such as data centers (Vertiv, 2016)—but are within the realm of normal experience and planning.

Instead, the committee focuses on large regional disruptions that last for several days or longer and cover a larger area, such as multiple service territories or even several states. Such long duration outages do occur, as shown in Figure 1.1 and discussed later in this chapter. Such events,

which can have profound system-wide effects, require much more attention than they have received to date from policy makers and every segment of society that depends on electric service. Because these effects are outside the realm of normal experience, it is difficult for people and organizations to imagine the possible harmful outcomes on the basis of real-world information about consequences. Reducing these harmful consequences of large-area, long-duration grid failures is a problem of imagination and incentives.

For shorter-duration outages, electricity users have an incentive to make their own preparations for resilience. A wide range of users do exactly that—with different levels of effort and cost depending on what they are willing to pay to avoid loss of vital services. Long-duration outages have much more profound impacts on society and require preparedness that is much more costly. Planning for such outages requires system-wide thinking because so much depends on the power grid, including all 16 critical infrastructure sectors.<sup>1</sup> As the grid becomes even more tightly integrated with other important economic and social activities, the need for this system-wide perspective will grow.

Water supply systems that provide potable water and treat wastewater are one example of critical infrastructure interdependency. Because the pumps are large, sometimes they do not have their own backup generators. Loss of grid power beyond a few hours can lead to depletion of gravity-fed reservoirs and tanks as well as a decline in pressurization of the distribution pipes. Usually the criticality of these pumps is handled through coordination with the electric distribution supplier to give those assets high priority during restoration—an option that may not be available during the

<sup>1</sup> The Department of Homeland Security designates the following 16 sectors to be critical to national security, national economics, or public health/safety: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation; and water and wastewater.



kinds of large-area, long-duration outages that are the focus of this report. Similarly, wastewater systems and particularly lift pumps are often critical if left off-line for too long. Sewage treatment often has enough storage to last for several days, but there have been cases where untreated effluent has been released directly to the environment in the aftermath of severe events.

Effective planning will require different strategies for different systems (NRC, 2012). And planning will require engaging actors—from first responders to the operators of critical infrastructures—who often do not work together adequately. Severe events and the corresponding shock, however, have inspired some of these different members of the private and public sector to work together more effectively—for example, during the aftermath of Superstorm Sandy when some parts of the tristate area lacked electric service and other infrastructure for more than a month.

This chapter looks at resilience from three perspectives: (1) incentives for actors to invest in resilience on their own, (2) planning methods that can improve how societies anticipate the effects of long-duration grid outages, and (3) approaches to designing electric power systems so they retain some or all of their function even when the larger grid has failed.

## INCENTIVES FOR PREPAREDNESS

By and large, the existing electric power grid has done a remarkable job of providing reliable electric power service. Moreover, existing users of electric power services generally have done a good job of investing where needed to make themselves more resilient when grid service is insufficient. This track record reflects the incentives at work on the actors who are relevant to planning and using grid electricity. Here the committee looks at those incentives because they help reveal places where additional efforts by industry, civil society, and government may be needed to anticipate and plan for large-scale grid outages. Such a perspective helps to expose the areas where failures to prepare are most likely—because the incentives to ensure resilience are weakest—and where additional policy action may be needed.

Surveys of existing electric power users reveal that there are huge variations in the willingness, ability, and need to pay for greater resilience; moreover, desire for resilience depends heavily on the expected duration of grid power outages. Table 5.1 shows results from one review of prior research on interruption costs of different duration and circumstances. The table is complex and busy, demonstrating huge variation (of several orders of magnitude) in the economic harm suffered by different types of customers for different types of outages. For example, the financial losses to large and medium commercial and industrial (C&I) customers are orders of magnitude larger than losses to either residential or small C&I customers. And while much is known about the impact of relatively short duration outages (<16 hours),

at present there is essentially no systematic research that provides such information for longer outages—let alone the large-area, long-duration outages that are the main subject of this study. Nonetheless, the existing research suggests that while, on the one hand, there are broader societal needs for more resilient power supply, on the other hand, cost-effective strategies must reflect that not all users need the same levels of resilience. This is particularly true for users and facilities that provide critical services such as hospitals, where using economic measures (e.g., willingness to pay) for resilient service may not be appropriate.

The incentive to become resilient is evident in the substantial investments that some power users make in obtaining backup supplies. For example, hospitals, data centers, and command posts for first responders all regularly install backup power systems. For smaller users, as well, there is extensive media coverage and advice—along with many vendor firms—that draw attention to the need for on-site power. Diesel generators are the technology of choice for this function; estimates compiled in the late 1990s suggest that the capacity of such generators in the United States was about 100 GW and growing at approximately 2 percent per year (Singh, 2001). Given the vital role of these generators in providing resilience, there has been ongoing attention to possible revision of standards for their reliability and environmental performance (Felder, 2007). There is also a substantial need for ongoing consumer education about the operation and safety of such devices since burns, fires, and especially carbon monoxide poisoning continue to be major problems.

The committee is concerned that, despite substantial investment in standby generators, awareness of the unreliability and other performance attributes of these systems remains highly uneven. According to Huber and Mills (2006), 1 percent of diesel generators at nuclear plants fail to start upon demand, while 15 percent of them fail after 24 hours of continuous operation. Consequently, nuclear sites have multiple redundant sources of backup power, and, in the wake of the Fukushima nuclear accident, the Nuclear Regulatory Commission has required additional investments in on-site power.<sup>2</sup> By contrast, the failure rates at start-up of hospital generators—which are much less well maintained in general and have fewer redundancies—are 10 times the rate of those in the nuclear industry (Mills, 2016). Similarly, there is low and uneven awareness of the challenges in obtaining fuel supplies in a long-duration outage, which presents a critical and underanalyzed risk.

**Finding:** Installing backup power systems alone is insufficient to improve resilience. These systems must be tested (i.e., started, operated) and maintained (e.g., cleaned) regularly so they function reliably during an outage. Relevant industry

<sup>2</sup> Following Fukushima, the Nuclear Regulatory Commission requires backup power for critical systems at nuclear power plants, which will likely cost the industry approximately \$4 billion (2016 dollars).

**TABLE 5.1** The Significant Variation in Estimated Financial Losses Suffered by Different Customer Classes Operating under Different Ambient Conditions as a Function of Varying Outage Duration

		Losses Based on Interruption Duration (\$)					
Timing of Interruption	Hours per Year (%)	Momentary	30 Minutes	1 Hour	4 Hours	8 Hours	16 Hours
<b>Medium and Large C&amp;I</b>							
Summer	33	16,172	18,861	21,850	46,546	96,252	186,983
Non-summer	67	11,342	13,431	15,781	35,915	77,998	154,731
Weighted Average		12,952	15,241	17,804	39,458	84,083	165,482
<b>Small C&amp;I</b>							
Summer Morning	8	461	569	692	1,798	4,073	7,409
Summer Afternoon	7	527	645	780	1,954	4,313	7,737
Summer Evening/Night	18	272	349	440	1,357	3,518	6,916
Non-summer Morning	17	549	687	848	2,350	5,592	10,452
Non-summer Afternoon	14	640	794	972	2,590	5,980	10,992
Non-summer Evening/Night	36	298	388	497	1,656	4,577	9,367
Weighted Average		412	520	647	1,880	4,690	9,055
<b>Residential</b>							
Summer Morning/Night	19	6.8	7.5	8.4	14.3	24.0	42.4
Summer Afternoon	7	4.3	4.9	5.5	9.8	17.7	31.1
Summer Evening	7	3.5	4.0	4.6	9.2	17.5	34.1
Non-summer Morning/Night	39	3.9	4.5	5.1	9.8	17.8	33.5
Non-summer Afternoon	14	2.3	2.7	3.1	6.2	12.1	23.7
Non-summer Evening	14	1.5	1.8	2.2	5.0	10.8	23.6
Weighted Average		3.9	4.5	5.1	9.5	17.2	32.4

NOTE: C&amp;I, commercial and industrial customers.

SOURCE: Sullivan et al. (2015).

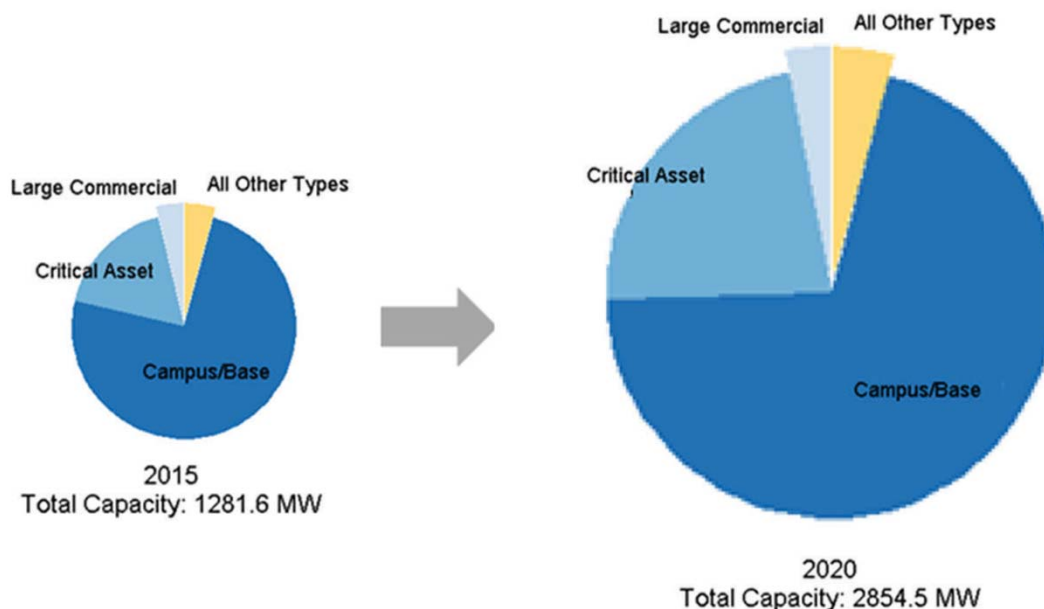
associations, and policy makers, government agencies, and regulators where appropriate, have an important role in disseminating information about the actual levels of reliability of backup units, as well as challenges obtaining fuel.

**Recommendation 5.1:** State emergency planning authorities should oversee a more regular and systematic testing of backup power generation equipment at critical facilities, such as hospitals and fire stations, and ensure that public safety officials include information related to electrical safety and responses to long-duration power outages in their public briefings. Those authorities should also periodically assess the costs and benefits of this testing program and use that information to prioritize sites for testing.

In addition to diesel generators—which are often connected to a single vital asset—there has been a steady rise in investment in microgrid systems (Hanna et al., 2017). These systems cover entire office complexes, campuses, and military bases, and, as shown in Figure 5.1, this segment of electricity infrastructure investment is expected to continue with substantial growth, which could have large implications

for the resilience of power users. While the logic for installing microgrids at such locations varies, usually the continued service of high-quality electricity even after macrogrid failure is dominant. Microgrids, especially the larger systems, are designed to allow for islanding in the event of macrogrid failure, although in practice very few actually operate or are even tested in that mode. Many microgrids embed renewable power generation systems—notably solar photovoltaics—and the financial case for larger microgrids typically hinges on the integration of natural gas-fired small turbines that utilize the waste heat for local heating and cooling. Later in this chapter, the committee will explore how new research and incentives could lead the users of microgrid systems to use this resource to increase resilience.

Over the past few years, there has also been a surge in installation of “behind the meter” on-site battery storage (see Figure 5.2 and the section titled “Near-Term Drivers of Change and Associated Challenges and Opportunities for Resilience” in Chapter 2). This surge in investment has been driven in part by direct subsidy—notably in California—and in part by fundamental improvements in battery technologies. As with microgrids, these on-site battery systems could



**FIGURE 5.1** Installation of microgrids in 2015 and expected growth to 2020.

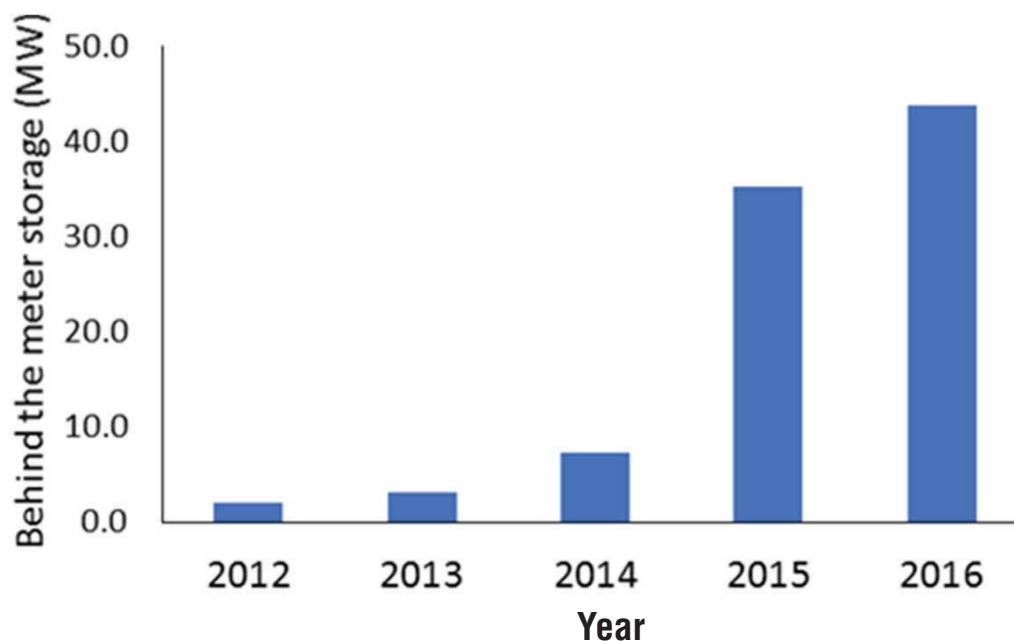
NOTE: Total U.S. electricity generation capacity in 2016 was more than 1,000 gigawatts.

SOURCE: GTM Research (2015).

in theory lead to higher resilience, but very few of these systems are actually designed for that purpose and none can supply power for periods of several days. Instead, these systems are sized to move small amounts of power—typically a fraction of total load just for an hour or two—from peak to non-peak periods to help C&I customers reduce the

charge they pay for peak electricity demand. If technological improvements make it possible to install much larger systems then such batteries could be material to improving resilience to long-duration grid outages.

Where power users have a self-incentive to invest adequately in resilience—and where they have adequate



**FIGURE 5.2** Installation of "behind the meter" battery storage systems.

SOURCE: GTM Research/ESA (2016), "U.S. Energy Storage Monitor."



**BOX 5.1****Consequences and Civic Response to Damage Caused by the Ice Storm of January 1998**

Ice storms are common in eastern Canada, with Ottawa and Montreal receiving freezing precipitation on an average of 12 to 17 days a year, but these events generally last only a few hours at a time. The January 1998 storm brought days of ice to an unexpectedly wide area of eastern Canada and the northeastern states, killing more than 40 people and causing large-scale, long-duration outages of electricity along with many other important impacts on infrastructure (NCEI, 1999).

Montreal was hit particularly hard. On January 9, much of Montreal temporarily lost its water supply after its filtration plant and pumping stations lost power (ICLR, 2013). Three out of the four major transmission lines in the area went off-line. If power had not been partially restored within hours, residents of the city would have been without potable water and firefighters would not have had water to put out fires—an outcome that forced officials to consider either evacuating the city or moving residents to facilities like Olympic Stadium, where water could be delivered by truck (Schneider, 1998). Early planning for such an outcome had not been contemplated seriously before—for example, through purchasing of on-site backup power plants—because the city had always been a priority customer of Hydro-Québec and officials thus assumed electricity would always be available (Schneider, 1998).

Even after power was restored, disruptions rippled through food supply chains, transportation, communications, and other economic activities. The storm occurred during the depths of winter and was followed by freezing weather and, 2 weeks later, by a snow storm of 8 to 16 inches that further slowed restoration (McDonnell, 1998). Along Montreal's south shore—which became known as the “triangle of darkness”—grid power remained out for 2 to 3 weeks following the storm (The Economist, 1998; Dupigny-Giroux, 2012). The commercial sector of Montreal was shut down for a week from January 9 through 16 to remove the debris and allow electrical crews to repair or rebuild the power grid in the island city (Dupigny-Giroux, 2012). Grocery stores across the area were unable to open or ran out of basic necessities, gas stations ran out of (or were unable to pump) fuel, and basic transport services were erratic—all leading to reports of a general feeling of vulnerability (Leslie, 1999; CBC, 2017; Murphy, 2009; Dupigny-Giroux, 2012; The Ottawa Citizen, 2016). All told, around 600,000 people moved out of their homes for the event, with 100,000 of them moving into temporary shelters to escape the cold (RMS, 2008). Restoration of grid services required assistance from utility crews drawn from across North America. The event prompted the largest peace time deployment of Canadian armed forces in history, with almost 16,000 troops assigned in the relief effort to help with cleanup, restoration, and evacuation.

information about the effects of their investments—no further policy incentives may be needed. By contrast, when the market fails—for example, when users are unaware of their exposure to grid failure, unaware of the synergistic consequences of grid failure, or unable themselves to afford or recoup the benefits of actions that could improve resilience if low probability events occur—then there may be a need for policy intervention. These failures are often evident where there are large-scale outages that affect a wide array of vital social services—as revealed, for example, by the long-duration power outage after the January 1998 ice storm described in Box 5.1. In contrast to many events whose intensity was predictable in ways that aided advance preparations, the extent and impact of this storm was largely unexpected. This is a characteristic of such storms since icing conditions depend critically on the vertical temperature profile in the atmosphere; a change of just a few degrees can make the difference among ice, rain, or snow. Such unexpected outcomes are particularly worrisome hazards for the grid since ice storms already account for many long-duration outages. With climate change, the areal extent and possible impacts of such icing events are likely to change although, as noted in Chapter 3, the nature of those changes remains uncertain.

The questions surrounding when and how policy makers intervene to encourage additional planning and investment around responses to grid failure raise many fundamental questions about the proper role of government. If government stands ready to provide support in the case of a long-duration grid failure, then the well-known “moral hazard” problems could undermine the incentive for users of electric power to make those investments themselves. While communities are largely left to make their own decisions about their willingness to plan for and invest in resilience, there may be broader social implications and possible unintended consequences from the totality of all these local choices made with reference to local interests.<sup>3</sup> Such societal concerns may create the need for policies to better harmonize or at least take these externalities into consideration. Indeed, better documentation and awareness of the metrics for grid reliability and resilience, discussed in earlier chapters, could make it much easier for market forces to function properly—for users of power services to become more fully aware of

<sup>3</sup> The issue of “moral hazard” arises if a community underinvests in protection for rare major events and then expects the broader society to cover its costs when such an event occurs.

their exposures to risk and thus more capable of obtaining the right level of resilience on their own.

Even once the right incentives are in place to invest in resilience, there may be organizational and cognitive barriers to action—especially for events that have never occurred or been imagined before. The committee believes that the largest challenges in creating resilience against the full effects of large-area, long-duration grid failures may lie with the system-wide consequences and interactions. Such problems are extremely difficult for organizations to anticipate and respond to effectively. Typically, organizations are structured to meet core missions and can be blind to, or find it very difficult to address, threats that arise in unexpected ways. Creating resilience against adverse system-wide effects requires that many different organizations coordinate and adopt solutions that might be far outside the normal scope of each organization individually. Where organizations do not have regular interaction and high levels of trust, collective action may be impossible.

The development of a coherent response that best serves the national interest requires laying a foundation for understanding the social value in resilience. Only then is it possible to evaluate whether the incentives of relevant actors will lead them to invest adequately in resilience. Only after establishing the social value in resilience is it possible to debate the degree of policy intervention needed to address the larger systemic impacts of large-area, long-duration outages.

**Finding:** The existing systems of incentives have generally been successful in encouraging proper levels of investment to address shorter-duration and limited-area outages. However, incentives for individuals and organizations to take steps to increase resilience against large-area, long-duration outages are a different matter. Developing national, regional, and local strategies to improve resilience against such outages requires two things: an assessment of the likelihood that disruptions will occur and a judgment about how much the various actors in society are prepared to invest in actions that lower the consequences of disruptions. At present, many communities, regulators, and grid operators do not have the information and/or incentives needed to make reasoned policy and operational decisions.

Knowing much more about what individuals and society are willing to pay to avoid the consequences of large grid failures of long duration is an important input to deciding whether and how to upgrade systems that can reduce impacts of a grid outage. Much of this knowledge is anecdotal from looking backward at such failures, such as from Hurricane Katrina, Superstorm Sandy, or the Northeast blackout of 2003. Most prior quantitative studies have only examined outages of much shorter duration. If these studies are to provide meaningful results, they will need to use state-of-the-art social science methods. Because different strategies may provide different insights, it would be prudent

to have separate independent groups undertake more than one study. Results from this work can be used to inform national, regional, and local decision making about resilience investment.

While individuals' willingness to pay is an important input to such decision making, considerations of broader social disruptions and of equity are also important. Some private actors may be willing to pay considerable amounts to assure their continued provision of electric power during events (or parts of them), but these actors typically lack incentive to make investments beyond their own needs. Others may be uninformed about the potential systemic consequences of long-duration outages. It is the role of government to assure the continued provision of critical social services and to provide access to basic power-dependent services to vulnerable groups such as disadvantaged communities or others that lack the financial mechanisms to assure their own resilience.

**Recommendation 5.2:** The National Association of Regulatory Utility Commissioners should work in coordination with the Department of Homeland Security, the Department of Energy, and the states to develop model guidance on how state regulators, utilities, and broader communities (where appropriate) might consider the equity and social implications of choices in the level and allocation of investments. These include investments in advanced control technologies capable of enabling continued supply to particular feeders or critical users that could mitigate the impacts of large-area, long-duration outages.

## PLANNING FOR GRID FAILURE

The remainder of this chapter examines how U.S. communities and the country as a whole can understand and implement an appropriate level of resilience in the event of a large outage of long duration. First, this section introduces planning for grid failure—so that consequences can be anticipated and responses organized. The following section discusses the design of infrastructures so that they themselves are more resilient to long-duration full or partial loss of grid services.

Planning requires information on the potential length and scope of large grid outages. That information can be gleaned partly by looking at past system outages and their coverage, summarized in Appendix E. These experiences suggest the magnitude of possible future outages. History in other countries is also helpful to consider because most modern grids reveal similar points of vulnerability. For example, the downtown area of Auckland, New Zealand, lost nearly all grid service for 5 weeks in the summer of 1998 when the four main cables serving the area failed in rapid succession. While each failure had its own individual causes, the events correlated and cascaded into a national crisis (Rennie, 1998).

Systems that should have been redundant instead were the source of additional stress—something that often happens in complex systems where all the interacting failure points are difficult to imagine in advance.

However, the past may be an inadequate guide because long-duration outages are rare events and the underlying structure, operation, and policies governing the grid might expose this vital infrastructure to even larger and longer outages than observed historically. It is important to do more to identify events that are “unthinkable” on the basis of historical experience but could occur with coordinated system-wide attacks on the grid and the many systems that it supports. While there are some public safety professionals and organizations that practice and train for such dark and disturbing work, these practices are neither widespread nor comprehensive enough to substantially improve the nation’s resilience to large-scale outages. Good imagination and planning begins with understanding the full range of possible outcomes for grid failure. The committee’s focus here is on planning for continuation of vital services in areas affected by a large-scale, long-duration outage, but it also notes that one important element of planning includes evacuation—in effect deciding that it may be more feasible to move populations in some areas than to provide emergency provisions.

While characterizing the real risks of grid failure will be difficult, an even more complex planning task involves understanding how prolonged full or partial failures of grid service could have compounding effects on other important public infrastructures and private services. Much of modern life depends on grid electricity, which is why the National Academy of Engineering named electricity as the single most important engineering achievement of the 20th century (NAE, 2017).

At present, planning for all types of hazards to public infrastructure is a disorganized and decentralized activity. Even in federal programs focused explicitly on increasing grid resilience, planning and implementation of research and policy responses are fragmented across federal agencies (GAO, 2017). It is impossible to describe all of the relevant efforts succinctly. Here the committee focuses on the role of the federal government and its National Preparedness System (NPS), whose broad aims are to prevent or speed recovery from a wide range of hazards that affect the security and resilience of the United States.<sup>4</sup> The NPS is organized by the Federal Emergency Management Agency (FEMA)—an arm of the Department of Homeland Security—to assess and plan for hazards to 12 vital emergency support functions, including energy, for which the Department of Energy (DOE) is responsible for primary agency support (FEMA, 2008). Table 5.2 shows the matrix of vital functions and the relevant federal agencies. It is an

intrinsically complex, messy, and organizationally stovepiped activity.

Because planning for grid failure is such an intrinsically complex and difficult task, it appears that very little of the FEMA- and DOE-led effort is devoted to imagining and preparing for the full systemic consequences of losing grid power over large areas for long period. Instead, by design, the framework shown in Table 5.2 is operational and aimed at clarifying which agencies will be focal points for receiving, collating, and distributing information to the rest of the federal government. Under this framework, for example, DOE is tasked with organizing information to produce estimates of restoration times, percentages, and priorities. In its role as the focal point, DOE is also expected to work with legal authorities to resolve matters of jurisdiction and grant waivers to expedite restoration processes, as discussed in Chapter 6. These are, for the most part, operational functions rather than forward-looking research and development or strategic planning. These patterns of stove piping and overlapping layers of jurisdiction extend from the federal to the regional, state, and local levels. Only during emergencies—events that politically and organizationally focus minds—does some semblance of more unified and strategic focus emerge, such as through the creation of joint field offices that unify the coordinating structures discussed in more detail in Chapter 6.

Because planning for the system-wide consequences of grid failure is such a daunting task, it is not surprising that the jurisdictions that seem to be doing a better job are those that have experienced such failures in the past. The tristate area of New York, New Jersey, and Connecticut in the aftermath of Superstorm Sandy is a good example, as shown in Box 5.2. Electricity outage disaster preparedness and response exercises such as “Clear Path 4” (DOE, 2016) are critical opportunities to gain experience and have great potential to be expanded. Experience transforms the unimaginable and seemingly impossible into a tangible reality. However, often the result is that planning efforts focus excessively on avoiding the same calamitous outcome rather than planning for a broader range of possible future events.

From the Sandy experience, the Canadian ice storm, and many others, it is clear that long-duration failures in grid power will occur. Even with a concerted effort in design and investment for continuity of some electric services—a topic discussed in the next section—much of the country is unprepared for long-duration outages. To the extent appropriate, resilience must begin with individual households and businesses preparing themselves for long-duration outages with adequate essential supplies—such as of food, water, medicine—to cover, at least, multi-day outages.

**Finding:** Existing planning systems are, by design, ill-suited for anticipating and considering the wide range of interactions between loss of grid power and other vital infrastructures and

<sup>4</sup> Presidential Policy Directive 8: National Preparedness. See <https://www.dhs.gov/presidential-policy-directive-8-national-preparedness>, accessed July 17, 2017.

**TABLE 5.2** The Federal Emergency Management Agency's Matrix Concept Illustrates the High Amount of Interagency and Interdepartmental Coordination Required for Assessing and Responding to Threats to the Nation's Vital Infrastructures

Department or Agency	Vital Emergency Support Functions											
	Transportation	Communications	Public Works and Engineering	Fire Fighting	Information and Planning	Mass Care	Resource Support	Health and Medical Services	USRT	HAZMAT	Food	Energy
Dept. of Agriculture	S	S	S	P	S	S	S	S	S	S	P	S
Dept. of Commerce		S	S	S	S		S			S		
Dept. of Defense	S	S	P	S	S	S	S	S	S	S	S	S
Dept. of Education					S							
Dept. of Energy					S		S	S		S		P
Dept. of Health and Human Services			S		S	S		P	S	S	S	
Housing and Urban Development						S						
Dept. of Interior		S	S	S	S					S		S
Dept. of Justice					S			S	S	S		
Dept. of Labor			S				S		S	S		
Dept. of State	S									S		S
Dept. of Transportation	P				S		S	S		S		S
Dept. of Treasury					S		S					
Dept. of Veteran			S			S	S	S				
Agency for International Development								S	S			
Administrative Resource Center					S	P		S			S	
Environmental Protection Agency			S	S	S			S		P	S	
Federal Communications Commission		S										
Federal Emergency Management Agency	S	S		S	P	S	S	S	P		S	
Government Services Agency	S	S			S	S	P	S			S	
Natl. Space and Aeronautics Admin.					S		S		S			
Natl. Clandestine Service		P			S		S	S				S
Nuclear Regulatory Commission					S					S		S
Office of Personnel Management							S					
Small Business Admin.					S							
Tennessee Valley Authority	S		S									S
U.S. Postal Service	S					S		S				

NOTE: P, principal coordinating agency; S, agencies supporting the principal coordinating agency; USRT, urban search and rescue.

SOURCE: FEMA (2008).

services for long-duration outages. These are intrinsically difficult tasks to perform both conceptually and organizationally. They require imagination and planning for interactions among multiple stresses on infrastructures and services that are rarely observed in the world.

For example, in the aftermath of a large regional storm, loss of grid power often leads to loss of reliable traffic control as well as obstruction of many roadways. These impede normal traffic flow and make it difficult for first responders to perform their tasks. The difficulties with first response,

**BOX 5.2****Superstorm Sandy: Preparation, Emergency Response, and Restoration of Services**

On October 29, 2012, Superstorm Sandy made landfall, leaving approximately 3.5 million of the 8.5 million homes and businesses in the tristate area without electricity. For 4 days prior to landfall, members of the Northeastern Mutual Assistance Group<sup>a</sup> were coordinating closely to reduce impacts and plan for restoration activities—and to reach out to other regions, such as the Midwest, to draw resources such as line crews and call center operators (EEI, 2013). Simultaneously, DOE worked to remove the red tape required for these outside crews to work in the impacted areas, as envisioned in the FEMA emergency preparedness process that had been established for the country just a year earlier (FEMA, 2013). A presidential state of emergency was declared a day before landfall, an action that further activated federal resources—such as the National Response Coordination Center (NRCC) that prepared five staging areas to preposition crews, vehicles, and 183 generators of various sizes. After landfall, as the extent of the damage became known, the NRCC also guided the Department of Defense to provide additional resources—such as airlifting 229 power-restoration vehicles and approximately 500 personnel to aid the region while the Army Corps of Engineers was tasked with pumping operations to facilitate restoration in flooded areas (FEMA, 2013). Within 2 days after landfall, 70,000 utility crewmen from around the country were working to restore the grid—by FEMA estimates, those workers replaced 4,500 poles, 2,100 transformers, 44 substations, and more than 400 miles of lines over the next 3 days (FEMA, 2013). With so many different federal agencies providing support, FEMA established the Energy Restoration Task Force on October 31 to help coordinate the federal effort—among many other functions, it coordinated the supply of 9.3 million gallons of fuel to New York and New Jersey for use by first responders and the continued operation of emergency generators (FEMA, 2013).

Since Superstorm Sandy, there have been extensive efforts by regulators and utilities to improve reliability of the grid and resilience of society—some of these efforts were triggered originally by Hurricane Irene, which hit the region the year before Sandy (FEMA, 2013). Concerning reliability, regulator orders and utility actions have identified critical power delivery systems that need hardening—such as raising the elevation of transformers at substations, adding supervisory control and data acquisition to substations, and installing equipment that will allow operators to isolate faulted areas and close circuits remotely that can keep more customers online. In the natural gas network, a massive effort has begun to replace cast iron mains and upgrade distribution systems. Public Service Electric and Gas—the largest utility in New Jersey, which saw 2 million of its 2.2 million customers lose power after Sandy—is in the midst of a regulator-approved \$1.2 billion “Energy Strong” program to protect its gas and electricity network. All told, in New Jersey alone, regulators have approved almost \$2 billion worth of investments in mitigation measures to guard against catastrophic storms and, more generally, upgrade the resilience of electric and gas systems.

Responses in New York were similar. In that state, 2.2 million customers lost power, and the two largest utilities (Consolidated Edison and Long Island Power Authority) spent \$1.2 billion to restore service while spending another \$1.7 billion after Sandy to harden their electricity, gas, and steam infrastructures.<sup>b</sup> In Connecticut, where the damage was much less relative to New York and New Jersey, relatively little federal help flowed—about 1 percent of the total federal funds spent after Sandy went to the state—and efforts focused less on recovery and hardening of infrastructure and more on helping homeowners displaced by the storm (Radelat, 2014).

Policy makers have also focused massive resources on improving resilience in the face of future power outages, although that task has required more complex coordination because few of the critical tasks for resilience map neatly onto existing policy structures. In New Jersey, the state's Board of Public Utilities in conjunction with the New Jersey Office of Emergency Management authored a Petroleum Fuel Task Force Plan. The New Jersey Board of Public Utilities is the lead agency for administering this new plan, which is intended to address fuel shortages or disruptions to the fuel distribution system in times of an emergency. More than 125 gas stations throughout the state have been equipped with emergency generators or electrical connections to accept a portable generator.

<sup>a</sup>Every region of the country has such mutual assistance groups.

<sup>b</sup>For regulatory action after Sandy, see, e.g., Cases 13-E-0030, 13-G-0031, and 13-S-0032 of the New York Department of Public Service.

in turn, magnify the humanitarian crises that result from the original storm event. Those difficulties compound into additional stresses on hospitals and public safety that consume their resources and make it more difficult to restore normal commercial operations. But even in such settings, it can be extremely difficult to anticipate how interactions among infrastructures lead to yet further interactions and harmful consequences that multiply as a grid outage event extends in time.

State and local emergency management organizations may not have sufficient understanding of electric power systems, which can slow down emergency power provision to critical facilities. In some states, such as California, organizations such as the California State Utility Emergency Association act as a liaison between critical infrastructure utilities and emergency management organizations. While several other states have similar programs, the practice is not widespread.



**Finding:** In every state, the governor is the ultimate authority responsible for overseeing disaster recovery and the mobilization of federal assistance. However, the states vary widely in the extent to which they are ready to perform these functions for long-duration grid outages. State and regional authorities would benefit from extending existing efforts to help identify common challenges and extend best practices—for example, the National Association of State Energy Officials' efforts to improve awareness and preparedness for large-scale disruptions to energy infrastructure (e.g., by holding events to share best practices and experiences managing fuel shortages that often accompany grid outages and other infrastructure failures [NASEO, 2016]).

The technology of distribution system operations increasingly allows power system operators, in the face of limited grid or local power supply, to select which distribution feeders to energize. Those feeders typically serve loads with very different levels of social criticality, such as hospitals or water treatment plants. Advanced control will make it possible to selectively supply and/or restore power to individual meters on a feeder, with subsequent or sequenced restoration of service to others on that feeder. It will also be possible to change the allocation of which meters to supply over time as circumstances and needs evolve. While presently there are relatively few demonstration projects and microgrids with these functionalities, there is significant potential to improve resilience through their wider adoption.

**Finding:** Technologies that allow for intelligent, adaptive islanding of the distribution system create new needs for planners to envision which feeders and users should be energized under different circumstances. Yet, that type of planning has been minimal, and little effort has been dedicated to anticipating how energizing feeders and select users might be adapted over the lifetime of the outage.

**Recommendation 5.3:** We recommend that the Department of Homeland Security, and the Department of Energy, as the energy sector-specific agency, develop and oversee a process to help regional and local planners envision potential system-wide effects of long-duration loss of grid power. While orchestrated at the federal level, success of this effort will require sustained engagement by regional and local authorities. Federal seed funding could support several such local or regional assessments.

Officials in regions that have experienced long-duration outages will likely be more motivated (see Box 5.2). In other regions, the Department of Homeland Security and others will need to mobilize support for taking these “imagine the unimaginable” activities seriously. The regulatory community's role in these efforts will be crucial. Public utility regulators in particular often have oversight over many

infrastructures and determine whether electric utilities may recover the costs associated with planning for the effects of long-duration outages of grid power.

**Recommendation 5.4:** The National Association of Regulatory Utility Commissioners, in consultation with the Department of Energy, the Department of Homeland Security, and the states, should develop guidance to state regulators and utilities on the following: (1) selective restoration options as they become available, (2) the factors that should be considered in making choices of which loads to serve, and (3) model recommendations that states and utilities can build upon and adapt to local circumstances. In developing these recommendations, attention should be paid to how the use of these new technical capabilities to energize particular feeders or grid-connected users might create evidence to justify wider deployment of such control and metering technologies.

Examples of factors that such guidance might consider include the power needs of first responder and other critical infrastructure systems, service to selected fuel and food suppliers, availability (or lack thereof) of privately supplied backup generation or other means to assure continued availability of electricity, and ability of specific populations to access basic services during prolonged outages.

The industry has done extraordinarily well at improving how the country responds to existing grid failures, a topic explored in more detail in Chapter 6. That said, a great deal of the effort needed to imagine and plan for the effects of long-duration outages sits outside the power industry in other organizations—such as the operators of water supply and treatment facilities and first responders. But industry, led by the North American Electric Reliability Corporation (NERC), should take a fresh look at whether the existing system of reliability standards adequately envisions cascading effects that could lead to long-duration outages. And the industry's central strategic organizations—notably the Edison Electric Institute, the American Public Power Institute, the National Rural Electric Cooperative Association, and NERC—should draw more attention to the need for society to plan for long-duration outages. This is important, even though such tasks may be uncomfortable for these organizations because they represent, to some degree, an awareness that the grid itself is more fragile than widely thought. At the same time, such self-driven industry efforts should improve awareness of the many ways that the grid system can be designed to allow more resilience, which is an area where there are highly varied experiences across existing U.S. utilities and other system operators.

Finally, much more attention is needed to engage the public in understanding the potential severity of large-area, long-duration blackouts and to improve public awareness and preparedness. The American Red Cross (2016) offers general guidance on how to prepare for power outages—with



supplies adequate for 3 days (assuming evacuation from home) or up to 2 weeks (assuming that homeowners stay at home). The Centers for Disease Control offer detailed guidance on food safety, noting that hazards to refrigerated food begin as early as 4 hours into a prolonged power outage; they also offer rudimentary strategies for disinfecting water (CDC, 2014). Many states also offer their own guidance tailored to local hazards—for example, Florida's advice focuses on the need for 3 days of supplies to ride through outages caused by hurricanes (Harrison, 2016). It is unclear how households around the nation respond to this advice, or what factors may drive households to achieve appropriate levels of preparedness. FEMA assesses individual preparedness on a regular basis, and the results suggest that preparedness is low and not improving rapidly (FEMA, 2016). Similarly, many households and businesses obtain equipment—such as portable generators—yet are unaware of how to operate these devices safely, how to procure fuel during extended outages, and how low the real levels of reliability of these devices are in practice.

## DESIGN

With better understanding of what society might be willing to pay to avoid or reduce the consequences of grid failure and equipped with better planning for how grid failure could affect other critical infrastructures, planners could then design systems so they are more resilient when grid power is lost. The committee looks at design from two related perspectives: (1) designing and deploying standby power systems, and (2) designing local power systems to provide higher customer resilience.

### Designing and Deploying Standby Power Systems

Many methods already exist to establish on-site power systems—often using components that are patched together in ad hoc ways—that can provide local service in the event of grid failure. These existing approaches should be practiced and improved. Most backup power systems rely on small gasoline, natural gas, and diesel-fired generators that are relatively easy to operate. Nonetheless, experience operating these systems is highly uneven around the country. Areas in which loss of grid power is more frequent are, as a general rule, better at imagining the impacts and thus better prepared.

These self-supplied systems may be ineffective in the case of long-duration, large-scale interruptions because backup systems are generally designed to run reliably for a few days at most; after that point, maintenance and fueling may be essential. However, during a large event that affects many interconnected public infrastructures, such services may be very challenging to obtain. During such outages, households and other non-expert users often devise their own ad hoc solutions that can lead to adverse side effects—for example, carbon monoxide poisoning from small generators run with

inadequate ventilation. Better information and oversight are needed to improve the availability, safety, and use of these power systems.

Many (if not most) of the emergency generators are not physical assets owned by government or even utilities. Instead, the government maintains contracts with the private sector to deliver equipment as needed. For example, the federal government maintains a small stockpile of portable generators at locations around the country, as well as much larger contracts for additional procurements that can be deployed during a major outage. It is poorly understood whether many of the contracts for provision of generators, fuel, and maintenance would prove to be robust under conditions that lead to sustained loss of grid power—conditions that might include natural disasters and cascading interactions between infrastructures under stress. For example, where delivery of these assets is envisioned by air, supporting facilities (e.g., airports, ground crews, and air traffic control) may be unavailable and roads may be impassable.

In addition to the contracts and stockpiles of mobile generators maintained by the federal government, there is potential to repurpose assets not traditionally used for power supply. Civilian and navy ships could provide a few tens of megawatts of emergency power to loads in coastal cities (Scott, 2006). Likewise, when they are equipped with appropriate interfaces or conversion kits, diesel electric locomotives can also be used to power communities located near railroad tracks. For example, Canada National Railway delivered multiple locomotives off-track to towns without power during the 1998 ice storm.

There are several other anecdotes of locomotives being used to supply power to critical loads during emergencies, and many train operators maintain conversion kits used to produce 60 Hz of alternating current power from locomotives. However, the availability of such conversion kits is likely limited, and it remains unclear how much load such non-traditional sources of emergency power could serve during actual blackout conditions (NRC, 2012). Nonetheless, such resources can augment federal emergency power operations that rely on conventional mobile generators.

**Finding:** The federal government maintains a small stockpile of portable generators and fuel, as well as contracts for additional procurements that can be deployed during a major outage. However, the quantity available in the event of a large outage is inadequate, probably by a large margin, and likely to remain that way. Furthermore, there is a lack of knowledge regarding the existence, load characteristics, and emergency power requirements of many critical facilities. During emergency operations, this can impede procurement, delivery, and installation of the proper equipment at the site. Also unknown is the ability to reliably obtain non-traditional sources of emergency power such as from train locomotives and ships.

**Recommendation 5.5:** The Department of Energy and the Department of Homeland Security should evaluate and recommend the best approach for getting critical facility managers to pre-register information about emergency power needs and available resources. Collecting this information in a centralized, accessible database will expedite provision of emergency power to critical facilities and help set priorities for allocating resources. The Emergency Power Facility Assessment Tool managed by the U.S. Army Corps of Engineers—a tool already in use but whose adequacy the committee was unable to assess completely—may prove to be a suitable platform. Once these informational resources are in place, periodic stress testing and evaluation are needed to ensure that they continue to provide reliable information.

It is crucial to increase community assessments of what will and will not work in the event of large outages of varying duration (including availability of liquid fuel and generators; power to refineries, gas stations, communication networks, and hospitals; local and regional availability of natural gas; workforce). These should be integrated with tabletop emergency planning exercises at the community, county, and state levels. FEMA provides some funding for state and local exercises. However, resilience to large-area, long-duration outages may not be adequately prioritized in existing state/local exercises, and greater emphasis could produce good models for systematic planning and operational assessments.

### Designing Local Power Systems to Provide Higher Customer Resilience

Beyond customer-owned sources of backup power, the power infrastructure, and distribution systems in particular, could be designed to operate more effectively when the bulk transmission parts of the grid fail. Many utilities are already installing self-healing and self-correcting distribution systems. These have ubiquitous sensors that can identify and isolate faults and use automated or remotely controlled switching to assure continuity of power to as many users as possible. For purposes of this chapter, what is important about these systems is that they blur the lines between reliability and resilience. When they work effectively, these automated distribution systems improve reliability of traditional grid service. But it is a small step to extend that logic to integration of electric infrastructure that is located on a customer's premises—for example, an intelligent microgrid that can island from or reconnect to the larger system as conditions require. Other examples include on-site battery storage at customers' residences, which combined with photovoltaics (PVs) could provide continuity of service in the event of grid failure (i.e., reliability) and also offer local support for the grid that can help avoid outages or expedite restoration (i.e., resilience). In terms of grid design and decentralization, these activities at the "edge" of the traditional grid are important technological and behavioral frontiers for the future

power system. At present, most of the capabilities—such as automated islanding and intelligent integration of local resources into utility distribution systems—are theoretical in nature and have not been tested at scale.

A particularly promising set of options related to improving resilience rests with various types of microgrids. It is crucial to understand how microgrids can enhance resilience by operating in self-islanding mode during long periods of grid failure. In that context, there are various classes of microgrids:

- *Building scale.* Nanogrids are small-scale microgrids feeding residential or commercial end users. During an outage, the nanogrid typically isolates from the distribution system, and individual energy resources (e.g., a rooftop PV system with battery energy storage, a local diesel generator, or a fuel cell) are used to power the local loads. At present, most of these small self-supply systems serve the purposes of improving reliability and saving customers' money through self-generation. Most of these systems are not designed to provide reliability for long-duration outages of the macrogrid, and many of these systems (e.g., at the residential level) are not designed to operate in islanded mode at all. Technically, however, many more of these systems could be designed with those capabilities.
- *Campus scale.* Microgrids are emerging as solutions for whole collections of buildings (e.g., college campuses or military facilities). All of these systems are designed with the capability of seamlessly connecting and disconnecting (i.e., islanding) from the macrogrid. Maintaining power at these locations—oases during emergency situations may be critical for safely riding through a catastrophic event. This is the fastest growth segment of microgrids in part because there are some customers willing to pay heavily for reliability (e.g., military bases) and in part because large-scale energy users can take advantage of combined heat and power efficiencies from burning natural gas in micro turbines (Hanna et al., 2017). For these latter users, dependence on natural gas supplies—which themselves may be compromised during events that lead to outage of the macrogrid—may be an extra source of vulnerability. Earthquakes that affect the power grid can also disrupt natural gas supplies. Extreme cold associated with ice storms can spike other demands for gas, such as heating, and leave less gas for power generation. Such systems, in many cases, are designed for islanding within the microgrids—so that critical services such as hospitals and sensitive scientific equipment are kept online even as the rest of the microgrid suffers graceful degradation in service.
- *Community scale.* Community-centric microgrids can be established by sharing individual end users' distributed energy resources (DERs)—a capability that exists

in principle but, so far, is rarely observed in reality. This functionality remains socially and technically challenging, as there are issues with safety, protection, controls, and metering.

**Finding:** There is enormous technical potential to using microgrids to make electric service more resilient in the face of loss of bulk grid power. This field of research and application is evolving quickly with new control systems, sensors, and distributed energy resources. This rapid evolution of the frontier of technical capabilities is opening a potentially wide gulf between the technical capabilities of microgrid systems and the real-world systems that are operational.

It is difficult to test microgrids and self-islanding distribution systems in real failure modes, especially if real-world events that lead to grid failure create many other forces that could erode the capabilities of self-islanded or microgrid systems. Variations in power quality could damage sensitive equipment needed for operation of these systems, as could physical stresses (e.g., trees, water, wind) that are correlated with the larger events that caused macrogrid failure in the first place. Too little is known about whether decentralization of the power grid will improve or degrade resilience of service under varying conditions. A highly decentralized and automated grid system that is still controlled by central authorities could prove to be a highly effective means of assuring resilient energy services even in the face of macrogrid failure. Or decentralization could actually amplify vulnerabilities in the grid system. Control systems may be unable to provide stability in the face of large numbers of local decisions made without the benefit of centralized authorities. Those systems might also fail in coordinated ways—for example, in case of cyber attack on the power infrastructure.

**Finding:** Many microgrids have been designed with continuous grid integration in mind, and users are hesitant to operate them in abnormal modes (e.g., islanded, or back-feeding power to the local utility) that could cause harm. Too little is known about whether decentralization of the power grid will improve or degrade resilience of service under varying conditions. A highly decentralized and automated grid system that is still controlled by central authorities could prove to be a highly effective means of assuring resilient energy services even in the face of macrogrid failure. Or, decentralization could actually amplify the vulnerabilities in the grid system.

**Recommendation 5.6:** The Department of Energy should support demonstration and a training facility (or facilities) for future microgrids that will allow utility engineers and non-utility microgrid operators to gain hands-on experience with islanding, operating, and restoring feeders (including microgrids). While the full need for training and experience—as well as possible adjustment in microgrid standards,

notably those developed by consensus under the Institute of Electrical and Electronics Engineers (e.g., 1547.4 and the 2030 family of standards, which are, at this writing, under revision)—is large, the committee envisions a small Department of Energy-backed program to establish best practices that could spread more widely across industry and the regulatory community.

As discussed in Chapter 2, today, in most states, regulatory and legal restrictions limit the ability of a microgrid to sell power to other entities or to move power across public thoroughfare unless it is operated by a traditional electric utility. At smaller scale, privately owned microgrids could offer significant advantages, even with existing rate structures that typically do not acknowledge the value such a system can provide to the grid (King and Morgan, 2007).

## DISTRIBUTION SYSTEM INNOVATIONS THAT COULD ENHANCE RESILIENCE

Today when the power goes out, individual customers are essentially on their own until service is restored. Homes and commercial facilities that are equipped with standby generators can disconnect from the grid and continue to operate with full or partial power. Users with microgrids—such as some campuses and military bases—can island from the grid and continue operations. Everyone else, even those customers with grid-connected PV systems, finds themselves in the dark. There are ways to enhance local resilience, such as by making PV inverters more visible and controllable, by facilitating development of small private microgrids, and by enabling utilities to operate islanded feeders.

### Increasing the Capabilities of Distributed Energy Resource Inverters

End users and utilities are investing in a wide array of DERs (e.g., PV arrays, wind turbines, battery storage), many of which are located on or near customers' premises. These resources could be used, in theory, to provide power to local loads even when the grid is unavailable. Typically, these local resources are interconnected with the grid through power electronic devices called inverters that convert the direct current output from many of these devices into alternating current. Integrating these resources into the grid has presented regulatory and technical challenges. Currently, these devices are required to automatically disconnect when the voltage and/or frequency at their terminals deviates outside of a normal range, indicating the presence of a fault somewhere on the grid. There are several reasons for this requirement, including safety of the line crews in the field and protection of equipment. However, because of the way inverters and their control systems are now implemented, this also results in cutting off the supply of power to the DER owner as well as to the grid. Given the rapidly increasing penetration of

DERs, it may often be desirable to keep these resources online during abnormal situations. Motivated by concerns related to the stability of the bulk power system, FERC has modified its small generator interconnection regulations to require that DERs have the ability to “ride through” momentary fluctuations of frequency or voltage.<sup>5</sup> In addition, the Institute for Electrical and Electronics Engineers is in the process of revising DER interconnection standards (IEEE, 2014), including guidelines for the intentional formation and operation of microgrids. These developments could have a positive impact on resilience during large-scale outages.

While it is not yet deployed at significant scale, technology is readily available to allow inverters to power local loads following automatic grid disconnection, making limited local power available to run refrigerators, freezers, and other critical loads.<sup>6</sup> In addition to increasing resilience and reliability for end-use customers, ongoing advances in inverter technology and modifications to interconnection regulations can be beneficial for keeping local loads at least partially energized during large-area, long-duration outages. Such advances can also be beneficial for utilities during restoration (see Chapter 6). With proper design and operating standards, DERs and advanced inverters could actively contribute to the stability and reliability of microgrids to power local loads without jeopardizing equipment or human safety. Nevertheless, individual states are in various stages of policy development related to inverter performance and interconnection of DERs.

**Recommendation 5.7:** Utility regulators and operating utilities that have not adopted standards similar to the Federal Energy Regulatory Commission’s ride-through capability requirements for small generators should assess their current interconnection standards as applicable to distributed energy resources, consider the costs of requiring new installations to use enhanced inverters, and determine the appropriate policy for promoting islanding and other related capabilities.

### Encouraging Private Microgrids

As explained in Chapter 2, in most states today, regulatory arrangements and laws granting distribution utilities exclusive service territories preclude private entities from constructing and operating microgrids if done in a manner that supplies power to an entity other than the owner of the microgrid or if that power is moved across a public thoroughfare. However, because many distributed generation (DG) systems display economies of scale (King, 2006), there may be sound economic justifications for customers to want

to operate some privately owned microgrids at a scale that serves several customers. Indeed, the military does this on many bases, at times with reliability benefits for non-military users as well. Microgrids have several advantages for the electricity grid; for example, they can provide electricity during peak-usage hours and therefore forestall the need for expensive upgrades in central generation, transmission, and distribution systems. They can also be used to improve power quality and reliability for local consumers (Neville, 2008). Finally, with proper arrangements they can serve local customers during power outages, consequently increasing the resilience of the grid. A potential advantage of facilitating the development of privately owned and operated microgrids is that this could considerably speed the pace of innovation (in much the way innovation was spurred after deregulation in the telecom industry).

**Recommendation 5.8:** The Department of Energy should work with the National Association of Regulatory Utility Commissioners and state regulators to undertake studies of the technical, economic, and regulatory changes necessary to allow development and operation of privately owned microgrids that serve multiple parties and/or cross public rights-of-way. These studies should also consider the potential consequences of such changes.

**Recommendation 5.9:** State legislatures and public utility commissions should explore economic, ratemaking, and other regulatory options for facilitating the development of private microgrids that provide resilience benefits. Rate structures can be developed to cover the costs of upgrading and maintaining grid assets while also recognizing and rewarding the benefits that distributed energy resources provide to the grid.

### Facilitating Utility-Operated Islanded Feeders

Traditional radial distribution feeders are designed only to move power from substations out to customers in one direction. More modern distribution systems that include distribution automation and intelligent bi-directional sectionalizing switches,<sup>7</sup> and other advanced distribution technologies, such as smart meters and micro-phasor measurement units, can reconfigure distribution system topology and feed distribution circuits from more than one location (Grijalva and Tariq, 2011; Grijalva et al., 2011). As the amount of utility and privately operated DG<sup>8</sup> on distribution systems grows, there is no technical reason why, during an extended

<sup>5</sup> FERC Order No. 828, 81, Fed. Reg. 50,290, 156 FERC ¶ 61,062 (2016).

<sup>6</sup> See, for example, the Outback FX 2.5kW 120VAC 24VDC 55A Sealed Inverter/Charger GTFX2524 from CivicSolar: <https://www.civicsolar.com/product/outback-gtfx2524-sealed-grid-tie-24v-25kw-inverter>, accessed July 13, 2017.

<sup>7</sup> See, for example, the IntelliRupter® PulseCloser® Fault Interrupter from the S&C Electric Company: [http://www.sandc.com/en/products-services/products/intellirupter-pulsecloser-fault-interrupter/](http://www.sandc.com/en/products-services/products/intellirupter-pulsecloser-fault-interrupter/http://www.sandc.com/en/products-services/products/intellirupter-pulsecloser-fault-interrupter/), accessed July 12, 2017.

<sup>8</sup> DG is a subset of DERs. DERs can include storage and non-generation resources.



outage, an intact distribution feeder could not be operated as an islanded micro-grid, supplying customers with limited critical electric service (Narayanan and Morgan, 2012). However, progress will be needed on a variety of technical and regulatory fronts. For example, as DG resources grow in size, simple “plug and play” arrangements are no longer feasible because issues of stability, as well as frequency and voltage control, become critical (Nazari et al., 2012; Nazari et al., 2013). Distribution systems with smart meters can drop customers before reconfiguring as an island, but issues of synchronizing DG resources and assuring adequate stability also need to be addressed (Nazari and Ilic, 2014). In most cases, it is unlikely that the amount of power available to an islanded feeder would be sufficient to meet all local loads. That means that methods would need to be developed to limit the load imposed by individual customers and perhaps to cycle supply among customers over time. Any operation of islanded feeders using DG resources must be planned and executed in a fashion that does not create a safety hazard for residents or utility repair crews.

Today, an inability to observe the details of what is going on (i.e., lack of visibility) in distribution systems is a significant technical barrier to the islanded operation of DGs and microgrids. Generally, this issue is lessened in transmission systems, as transmission systems typically have greater visibility. During a power outage, transmission system operators can often readily and accurately identify most fault(s) and isolate them from the rest of the grid. Thus, the rest of the system can continue its normal operation while line crews work to repair the isolated part of the grid in a safe manner. If utilities undertake a similar approach for distribution systems and implement smart meters and micro-phasor measurement units in distribution systems, or at least at the points of interconnection of DGs/microgrids, they can identify energized lines during outages and isolate them to ensure line crew safety, while serving critical loads.

**Recommendation 5.10:** Utilities that have already implemented smart meters and advanced distribution systems with sectionalizing switches should explore the feasibility of establishing contractual and billing agreements with private owners of distributed resources and developing the ability to operate intact islanded feeders as islanded microgrids powered by utility- and customer-owned generating resources to supply limited power to critical loads during large grid outages of long duration.

**Recommendation 5.11:** Utility regulators and non-governmental entities should undertake studies to develop guidance on how best to compensate the owners of distributed generation resources who are prepared to commit a portion of their distributed generation capacity to serve islanded feeders in the event of large outages of long duration. Additionally, the National Association of Regulatory Utility Commissioners

should establish a working group to advise members on the issues they will likely have to address as the possibility grows that some utilities or customers may wish to be able to operate islanded feeders during large outages of long duration.

### Facilitating Emergency Use of Hybrid and Fuel Cell Vehicles for Backup Power

With appropriate inverters, plug-in hybrid electric vehicles and fuel cell vehicles are effectively mobile generators that customers could use to provide emergency power to critical loads in their homes, and in theory to an islanded feeder, during a major outage. Like other mobile generators, this service depends on continued availability of fuel, whether natural gas, gasoline, or something similar. Battery electric vehicles with no combustion system only store modest amounts of energy (i.e., 80 kWh at the high end), which would likely be exhausted early in the course of a large-area, long-duration outage. Thus, purely electric vehicles do not offer the same level of resilience benefit for homeowners but could be coupled with DG such as PVs. Inverters designed for vehicle-to-home power transfer have not entered the market in the United States, although there are numerous demonstration projects, in part because of technical, economic, and liability questions that must be negotiated among grid operators, homeowners, and vehicle manufacturers.

**Recommendation 5.12:** The Department of Energy should work with the manufacturers of plug-in hybrid electric and fuel cell vehicles to study how such vehicles might be used as distributed sources of emergency power.

## REFERENCES

- American Red Cross. 2016. “Power Outage Safety.” <http://www.redcross.org/get-help/prepare-for-emergencies/types-of-emergencies/power-outage/#Prepare-in-Advance>. Accessed July 11, 2017.
- Briggs and Stratton. 2015. “Briggs & Stratton Corporation Harris Poll Survey: How Homeowners Prepare for Power Outages.” [https://www.briggsandstratton.com/na/en\\_us/news-room/basco-harris-poll-survey-regarding-power-outages.html](https://www.briggsandstratton.com/na/en_us/news-room/basco-harris-poll-survey-regarding-power-outages.html). Accessed May 31, 2015.
- CBC (Canadian Broadcasting Corporation). 2017. “The Ice Storm of 1998.” <http://www.cbc.ca/archives/topic/the-ice-storm-of-1998>. Accessed March 30, 2017.
- CDC (Centers for Disease Control and Prevention). 2014. “Natural Disasters and Severe Weather.” <https://www.cdc.gov/disasters/poweroutage/needtoknow.html>. Accessed May 31, 2017.
- DOE (Department of Energy). 2016. *Clear Path IV Energy-Focused Disaster Response Exercise: Exercise Summary Report*. [https://energy.gov/sites/prod/files/2016/08/f33/ClearPathIV\\_Exercise%20Summary%20Report\\_Public%20Release.pdf](https://energy.gov/sites/prod/files/2016/08/f33/ClearPathIV_Exercise%20Summary%20Report_Public%20Release.pdf).
- Dupigny-Giroux, L.A. 2012. USA impacts and consequences of the ice storm of 1998 for the North American north-east. *Weather* 55(1): 7–15.
- Eaton. 2016. *Blackout Tracker: United States Annual Report*. [http://images.electricalsector.eaton.com/Web/EatonElectrical/%7Bc9381362-7f37-4a86-921f-83e72e8792e1%7D\\_Blackout\\_Tracker\\_US\\_2016\\_Annual\\_Report.pdf](http://images.electricalsector.eaton.com/Web/EatonElectrical/%7Bc9381362-7f37-4a86-921f-83e72e8792e1%7D_Blackout_Tracker_US_2016_Annual_Report.pdf).

- EEI (Edison Electric Institute). 2013. "Mutual Assistance." <http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Pages/default.aspx>. Accessed December 15, 2016.
- Felder, F.A. 2007. *New Performance-Based Standards for Standby Power: Re-examining Policies to Address Changing Power Needs*. <http://www.cleaneenergy.org/wp-content/uploads/New-Performance-based-Standards-for-Standby-Power.pdf>.
- FEMA (Federal Emergency Management Agency). 2008. *Emergency Support Function Annexes: Introduction*. [https://www.fema.gov/media-library-data/20130726-1825-25045-0604/emergency\\_support\\_function\\_annexes\\_introduction\\_2008\\_.pdf](https://www.fema.gov/media-library-data/20130726-1825-25045-0604/emergency_support_function_annexes_introduction_2008_.pdf). Accessed July 11, 2017.
- FEMA. 2013. *Superstorm Sandy After Action Report*. [https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy\\_fema\\_aar.pdf](https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf).
- FEMA. 2016. "Research: Citizen Preparedness Surveys Database." <https://www.ready.gov/research>. Accessed July 11, 2017.
- GAO (Government Accountability Office). 2017. *Electricity: Federal Efforts to Enhance Grid Resilience*, GAO-17-153. <https://www.gao.gov/assets/690/682270.pdf>.
- Grijalva, S., and M.U. Tariq. 2011. Prosumer-based smart grid architecture enables a flat, sustainable electricity industry. In *Innovative Smart Grid Technologies*. Proceedings of the IEEE Power and Energy Society General Meeting, Anaheim, Calif., Jan 17–19.
- Grijalva, S., M. Costley, and N. Ainsworth. 2011. Prosumer-based control architecture for the future electricity grid. In *Control Applications*. Proceedings of the IEEE International Conference on Control Applications, Denver, Colo., September 28–30.
- GTM Research (Greentech Media Research). 2015. *North American Microgrids 2015: Advancing Beyond Local Energy Optimization*. <https://www.greentechmedia.com/research/report/north-american-microgrids-2015>. Accessed July 17, 2017.
- GTM/ESA (Energy Storage Association). 2016. "U.S. Energy Storage Monitor." <https://www.greentechmedia.com/research/subscription/u.s.-energy-storage-monitor>. Accessed July 17, 2017.
- Hanna, R., M. Ghonima, J. Kleissl, G. Tynan, and D.G. Victor. 2017. Evaluating business models for microgrids: Interactions of technology and policy. *Energy Policy* 103: 47–61.
- Harrison, C. 2016. "The Essential Guide to Hurricane Preparedness." <http://www.stateofflorida.com/articles/hurricane-preparedness-guide.aspx>. Accessed December 30, 2016.
- Huber, P., and M. Mills. 2006. *The Bottomless Well: The Twilight of Fuel, the Virtue of Waste, and Why We Will Never Run Out of Energy*. New York: Basic Books.
- ICLR (Institute for Catastrophic Loss Reduction). 2013. "Ice Storm 98: An Ice Storm Chronology." <http://www.iclr.org/icestorm98chrono.html>. Accessed December 30, 2016.
- IEEE (Institute for Electrical and Electronics Engineers). 2014. *IEEE 1547 Standard for Interconnecting Distributed Resources with Electric Power Systems*. [http://grouper.ieee.org/groups/sc21/1547/1547\\_index.html](http://grouper.ieee.org/groups/sc21/1547/1547_index.html). Accessed July 11, 2017.
- King, D.E. 2006. Electric Power Microgrids: Opportunities and challenges for an emerging distributed energy architecture [PhD Thesis]. Carnegie Mellon University, Pittsburgh, Pa.
- King, D.E., and M.G. Morgan. 2007. Customer-focused assessment of electric power microgrids. *Journal of Energy Engineering* 133:3.
- Leslie, J. 1999. "Powerless." *Wired Magazine*, April 1. <https://www.wired.com/1999/04/blackout/>. Accessed July 11, 2017.
- McDonnell, S. 1998. "Diary of a Disaster: 1998 Ice Storm." <http://www.imiuru.com/icestormdiary/1pages/MoreDiary.html>. Accessed December 15, 2016.
- Mills, M. 2016. *Exposed: How America's Electric Grids are Becoming Greener, Smarter, and More Vulnerable*. New York: Manhattan Institute.
- Murphy, R. 2009. *Leadership in Disaster: Learning for a Future with Global Climate Change*. Québec, Canada: McGill-Queens University Press.
- NAE (National Academy of Engineering). 2017. "Greatest Engineering Achievements of the 20th Century." <http://www.greatestachievements.org/>. Accessed July 13, 2017.
- Narayanan, A., and M.G. Morgan. 2012. Sustaining critical social services during extended regional power blackouts. *Risk Analysis* 32: 1183–1193.
- NASEO (National Association of State Energy Officials). 2016. "Western Regional Emergency Fuel Coordination Meeting." <http://www.naseo.org/event?EventID=1435>. Accessed July 11, 2017.
- Nazari, M.H., and M. Ilic. 2014. Dynamic modelling and control of distribution energy systems: Comparison with transmission power systems. *The Institution of Engineering and Technology Generation, Transmission, and Distribution* 8(1): 26–34.
- Nazari, M.H., M. Ilic, and J.P. Lopes. 2012. Small-signal stability and decentralized control design for electric energy systems with large penetration of distributed generators. *Control Engineering Practice* 20(9): 823–831.
- Nazari, M.H., M. Ilic, and M.G. Morgan. 2013. "Toward Model-based Policy Design for Reliable and Efficient Integration of Distributed Generators." Presented at the IEEE PES General Meeting, Vancouver, British Columbia, July.
- NCEI (National Centers for Environmental Information). 1999. "Eastern U.S. Flooding and Ice Storm." <https://www.ncdc.noaa.gov/oa/reports/janstorm/janstorm.html>. Accessed December 15, 2016.
- Neville, A. 2008. "Microgrids Promise Improved Power Quality and Reliability." *Power Magazine*, June 15. <http://www.powermag.com/microgrids-promise-improved-power-quality-and-reliability/>. Accessed February 8, 2017.
- NRC (National Research Council). 2012. *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press.
- Radelat, A. 2014. "Feds give Connecticut relatively little for recovery from Sandy." *CT Mirror*, June 20. <http://ctmirror.org/2014/06/20/feds-give-connecticut-little-to-recover-from-sandy/>. Accessed July 11, 2017.
- Rennie, H. 1998. "Auckland Power Supply Failure." <https://web.archive.org/web/20090307230605/http://www.med.govt.nz/templates/Page12136.aspx>. Accessed December 15, 2016.
- RMS (Risk Management Solutions). 2008. *The 1998 Ice Storm: 10-Year Retrospective*. [http://forms2.rms.com/rs/729-DJX-565/images/wtr\\_1998\\_ice\\_storm\\_10\\_retrospective.pdf](http://forms2.rms.com/rs/729-DJX-565/images/wtr_1998_ice_storm_10_retrospective.pdf).
- Ryan, B., R.C. Franklin, F.M. Burkle, P. Aitken, E. Smith, K. Watt, and P. Leggat. 2015. Identifying and describing the impact of cyclone, storm and flood related disasters on treatment management, care and exacerbations of non-communicable diseases and the implications for public health. *PLOS Currents Disasters*. Edition 1, September 28.
- Schneider, H. 1998. "Close Call Spurs Disaster Plan Review." *The Washington Post*, January 25.
- Scott, R.D. 2006. *Ship to Shore Power: US Navy Humanitarian Relief?* [https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-691-seminar-in-electric-power-systems-spring-2006/projects/ship\\_to\\_shore.pdf](https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-691-seminar-in-electric-power-systems-spring-2006/projects/ship_to_shore.pdf).
- Singh, V. 2001. Blending wind and solar into the diesel generator market. *Renewable Energy Policy Project* 12.
- Sullivan, M., J. Schellenberg, and M. Blundell. 2015. *Updated Value of Service Reliability Estimates for Electric Utility Customers in the United States*. LBNL-6941E. <https://emp.lbl.gov/sites/all/files/lbnl-6941e.pdf>.
- The Economist. 1998. "After the storm, the clearing-up," January 15. <http://www.economist.com/node/110924>. Accessed July 11, 2017.
- The Ottawa Citizen. 2016. "Remember The Ice Storm of '98? It Was the Most Devastating and Least Ferocious of Canadian Disasters," February 24. <http://ottawacitizen.com/news/local-news/remember-the-ice-storm-of-98-it-was-the-most-devastating-and-least-ferocious-of-disasters>. Accessed July 11, 2017.
- Vertiv. 2016. "Benchmark Series." <https://www.vertivco.com/en-us/insights/articles/pr-campaigns-reports/benchmark-series/>. Accessed July 11, 2017.



# 6

## Restoring Grid Function After a Major Disruption

### INTRODUCTION

This chapter discusses the post-event system restoration and the learning phases of the resilience model laid out in Figure 1.2. The committee first introduces a general model for electricity system restoration after a large-area, long-duration outage and then discusses restoration for several classes of disruptions based on the type of damage caused. This organization is based on the recognition that restoration activities proceed differently based on different types of outages—following some events, utility operators will have no situational awareness to guide their deployments; whereas other events may leave monitoring systems intact but overwhelm stockpiled resources. The chapter includes recommendations for improving the restoration process and for improving post-incident investigation to better learn from each experience to improve future performance.

### GENERAL MODEL FOR ELECTRICITY RESTORATION

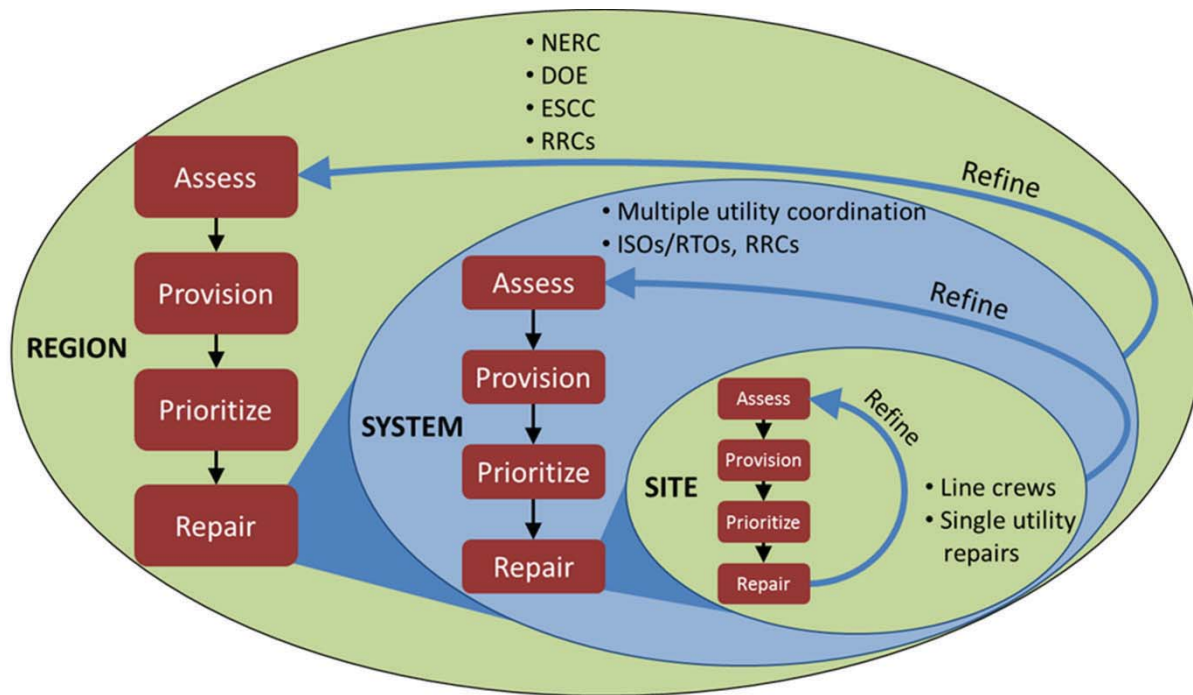
Following a large-area, long-duration outage, electricity system operators set priorities and work across organizational boundaries to bring the system back online as quickly as possible through a series of restoration activities. While the exact steps and procedures for restoration vary depending on the nature of the outage and the damage incurred, electricity providers follow four general restoration steps:

1. Assess the extent, locations, and severity of damage to the electricity system;
2. Provide the physical and human resources required for repairs;
3. Prioritize sites/components for repair based on factors including the criticality of the load and the availability of resources to complete the needed repairs; and
4. Implement the needed repairs and reassess system state.

As shown in Figure 6.1, these general processes are carried out simultaneously by different organizations operating

at different scales across all elements of the power system. Many of these organizations have their own restoration plans, spanning those from individual distribution cooperatives such as Cuivre River Electric Cooperative in Missouri (CREC, 2016), to large investor-owned utilities such as New York State Electric and Gas Corporation and Rochester Gas and Electric Corporation (NYSEG and RGEC, 2016), to independent system operators such as PJM (2016). Organizations frequently involved in electricity restoration include not only electricity system operators (i.e., distribution, transmission, and generation utilities and independent system operators), but also emergency management officials from city, county, state, and federal organizations, including the Federal Emergency Management Agency (FEMA), the Department of Energy (DOE), state emergency management agencies, the National Guard, and in some cases even the Department of Defense. Depending on the circumstances, organizations that operate far afield of the utility sector may be called on when they offer special capabilities—for example, the deployment of the U.S. Air Force to transport bucket trucks by air from California to New York in response to Superstorm Sandy. Effective restoration rests on the collaboration and cooperation of myriad organizations and individuals of different skills. Various mutual assistance agreements provide additional resources to extend the reach of the restoration across geographic and organizational boundaries. The restoration work itself is dependent on the skills and resources of the line and electrician crews deployed by the local utilities.

Coordination and communication among these groups is challenging, in part because each group has different responsibilities and boundaries within which it operates. Knowledge of local conditions and needs is greatest at the site level and diminishes with increasing scale, whereas understanding of systemic risks and critical needs may be greater at the regional scale. Thus, information must flow in both directions, and, while prior agreements can help considerably, communication channels specific to the actors and hazards involved are often established in an ad hoc manner.



**FIGURE 6.1** Illustration of the general processes of restoration that occur on multiple levels by different institutions with responsibility for electricity restoration.

NOTE: NERC, North American Electric Reliability Corporation; DOE, Department of Energy; ESCC, Electricity Subsector Coordinating Council; RRC, regional reliability coordinator; ISO, independent system operator; RTO, regional transmission organization.

These communications must be agile and flexible, evolving in response to changing conditions and the shifting composition of the restoration team. Communication is partly a technical issue and partly an organizational issue—for example, determining who should have access to information. In recent storms such as Superstorm Sandy, coordinating the dispatch and routing of crews through damaged and flooded areas was a challenge, and crews were sometimes delayed because they could not reach affected areas.

Beyond identifying a specific threat to the electricity system, key utility CEOs and federal decision makers meet through the Electricity Subsector Coordinating Council to plan for national-level incidents and maintain open communication channels (ESCC, 2016). This lays a good foundation for restoration activities, but an agile approach is necessary to deal with specific circumstances. Exercises are critical, although exercises alone will not address an actual event in all regards. Nonetheless, practice and associated learning will improve reactions during actual response.

During a major disaster, the states coordinate all first responder and restoration activities. For large incidents, when federal resources are warranted and mobilized, the National Response Framework provides the organizational structure, FEMA coordinates federal assets, and DOE is appointed the energy-sector lead agency (DHS, 2016). In preparation for or response to major outages, DOE will

staff local and headquarters operations centers to coordinate federal actions that expedite electricity system restoration, working closely with the electricity organizations involved and other responders. Examples of DOE action include waiving federal transportation regulations on the time trucks can drive continuously so as to bring necessary equipment to the affected area more rapidly.

When a physical disruption of the power system occurs, it is important that utility repair crews be able to gain rapid access to damaged substations and other facilities so they can safely isolate and de-energize hazardous components, retain and gain access to emergency communication equipment and supplies, promptly assess damage, and start the process of restoration. In that context, the issue of working with law enforcement to gain access becomes critical, both for reasons of safety and because supplying power can be a key component of disaster recovery and avoiding further risks and damages.

One possible strategy could be to designate selected utility personnel as “first responders.” While there have been efforts to move in this direction, they have become stalled because doing so could raise potential issues of liability, perhaps placing crews under state control or even requiring crews to divert their efforts away from electricity-related activities. The Edison Electric Institute (EEI) and others have been working at high levels to reach informal agreements

about achieving access. One problem with such an informal approach is that, without official credentialing, other first responders on the ground may not be aware of such arrangements and serious delays in access can occur. The situation could become even more complicated in the event of a major terrorist attack on substations or other critical grid facilities that might be designated as “crime scenes.” A similar situation could arise in the wake of a cyber attack where affected systems might be considered evidence.

**Finding:** When major physical damage occurs in the power grid, it is important that utility repair crews be able to gain rapid access. Due to a lack of standing arrangements with law enforcement and other first responders, this is not always possible; informal high-level agreements about access do not always result in smooth operations among key personnel on the ground.

**Recommendation 6.1:** The Department of Homeland Security in collaboration with the Department of Energy should redouble efforts to work with utilities and national, state, and local law enforcement to develop formal arrangements (such as designating selected utility personnel as “first responders”) that credential selected utility personnel to allow prompt utility access to damaged facilities across jurisdictional boundaries. Such agreements should address issues such as indemnity, liability, and the risk of diverting the mission and assets of utility crews to other non-power system objectives.

### Utility Planning for Restoration from Major Disruptions

Utilities are well practiced at recovering from localized damage to the grid and helping to restore the system outside their service areas following large events. From line crews to executives, utilities are familiar with recovery from regional natural hazards; they have developed restoration plans and allocated resources for recovery operations. Some utilities equip bucket trucks with mobile generators and communications equipment that allow line crews to maintain contact and proceed with repairs even when the bulk grid and communications infrastructures are down. When damages to the physical system exceed the hardware or human resources of a single utility, mutual assistance agreements (MAAs) are used widely throughout the industry to expedite sharing of crews and equipment among utilities. For larger events, crews and equipment are often brought in from thousands of miles away to aid restoration efforts in affected areas. Following Superstorm Sandy, the EEI developed a National Response Event framework for coordinating regional MAAs across the United States (EEI, 2016). Although the National Response Event framework has not yet been tested, it is designed to help prioritize and expedite dispatch of line crews and resources on a national scale with a comprehensive understanding of damages and restoration efforts.

Utility restoration plans emphasize advanced planning, communication, training, and continual refinement and improvement. Restoration plans are drilled by utilities and externally reviewed by the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC), and regional reliability organizations. One recent voluntary review found that participating organizations maintained system restoration plans that were thorough and highly detailed; however, opportunities for improvement remain (NERC, 2016a). For example, restoration plans may make key assumptions about the availability of certain assets (e.g., that a pre-identified black-start transmission corridor is operational) that, depending on the extent of damage, may not hold true.

Depending on the hazard, it may be possible for utilities to strategically deploy assets and for state and federal agencies to be mobilized in advance of the event. For example, utilities operating along the Gulf Coast have a long history of anticipating and recovering from large storms that cause extensive damage, and their restoration plans and activities reflect this history. In the week before Hurricane Katrina, Southern Company and its operating subsidiaries in Mississippi and Alabama spent more than \$7 million pre-staging personnel and supplies, including catering and amenities for restoration workers, many of whose families were directly impacted by the storm (Ball, 2006). The arrival of Superstorm Sandy was preceded by a large mobilization of assets by utilities and the federal government (Fugate, 2012; Lacey, 2014). Vermont Electric Power Company's Weather Analytics Center provides highly accurate weather forecasts that the utility uses to pre-position restoration crews and assets (NASEM, 2016). Developing additional technologies and strategies to improve pre-positioning of restoration assets remains an important area for additional effort.

The process of electricity system restoration begins long before a specific event or threat is identified, through extensive planning, training, drilling, and pre-positioning of assets, and continues after all service has been restored, through continual refinement of a utility's restoration plans. Fundamental to all restoration planning is an unresolvable uncertainty: the exact nature of damage cannot be known before an event occurs, and restoration plans must simultaneously be specific and actionable for utility personnel yet general enough to accommodate diverse potential scenarios. Thus there is no uniform, repeatable process for restoration that extends beyond a single event. There are many post-action reports from major outages that describe the event, how it was addressed by whom, and lessons learned. By systematically evaluating previous experiences and more openly sharing information about recovery from major outages, utilities have an opportunity to identify and share best practices. While such analysis is conducted on behalf of transmission utilities at the North American Transmission Forum, these assessments do not cover distribution utilities.

**Recommendation 6.2:** With support and encouragement from relevant state and federal regulatory agencies, the Department of Energy and utilities should continue to work together to analyze past large-area, long-duration outages to identify common elements and processes for system restoration and define best practices that can be shared broadly throughout the electricity industry. The committee notes that progress has been made with the ongoing efforts of the Electricity Subsector Coordinating Council, which provides a good framework for expanded coordination and sharing of best practices.

### Black-Start Recovery Plans

Large generation and transmission operators maintain restoration and recovery plans for energizing the high-voltage transmission system following a large-area, long-duration outage. Most generation facilities require electricity for operation, so if generators have gone off-line, these plans begin by starting selected “black-start” generators that do not require power from the larger grid to function. There are almost always functioning areas of the grid adjacent to the area experiencing an outage, and service can be most effectively restored from the edges of the blacked-out areas. If this is not the case, then black-start generators must first supply power to nuclear plants for safe shutdown before providing power to other generating stations. While black-start plans are difficult or impossible to practice (because doing so would require shutting down the grid), restoration plans provide detailed information on black-start resources in a utility’s service area, identify the priority loads and transmission corridors that the utility will bring power to first, and provide operators with key contact information. The priority loads for restoring the electricity system are other non-black-start generation plants—particularly nuclear plants that require external power—as well as natural gas pumping stations that maintain pressure in pipelines and provide fuel for natural gas generators to come online.

As generators and transmission corridors become energized, power is provided to distribution circuits—with priority given to known critical loads such as hospitals and repairs that restore service to the most customers. As restoration progresses, more generators are connected and resynchronized until service is restored to more loads. In some cases, this restoration may involve forming “islands” of electrical service: multiple smaller regions maintain balance of generation and load independent of the remaining grid and are then subsequently synchronized to the remaining system (PJM, 2016). Depending on how quickly generators are restored, some low-priority loads may need to remain off-line as the electricity providers will ration available supply to meet prioritized demand requirements. The time required to complete this process depends significantly on the damage to the infrastructure, the amount of data and information available, and the availability of restoration resources.

The Electric Power Research Institute (EPRI) has developed generic restoration milestones as well as a comprehensive

methodology for power system restoration based on these milestones. It is also developing and demonstrating a prototype decision support tool for evaluating system restoration strategies (EPRI, 2010). The Optimal Black-Start Capability tool can be used by utilities to evaluate the suitability of available black-start capable units and plan optimal locations and capacity levels for new black-start units.

The restoration process is highly dependent on the topology of the transmission and distribution networks, which determine the sequence of restoration starting from the black-start generators. If in the future the generation resources are more decentralized and placed on the distribution feeders, the topology of the grid, and hence the restoration process, becomes more complex. However, the smaller generation resources closer to the loads can make the generation-load balance easier during restoration, provided that these generators (and even responsive loads) have adequate controllability. With the higher penetrations of distributed energy resources (DERs), the restoration process will need to be rethought.

### Opportunities to Include Distributed Energy Resources in Restoration and Black Start

Traditionally, black-start plans have focused entirely on large, centralized utility generation assets. As the grid evolves to include larger amounts of DERs more broadly, it becomes important to consider the role these resources might play in the context of black start. The benefits and impacts of DERs will vary by geographic region because some distribution utilities have a higher penetration of DER assets than other areas. Additionally, some distributed generation and other assets are monitored and controlled by third-party entities other than the utility or grid operator because state policies do not allow these utilities to operate behind the meter. At low levels of penetration, DERs should simply be operated in ways that do not interfere with any needed black-start operations. As noted in Chapter 5, with appropriate system upgrades and institutional arrangements, microgrids and DERs could provide islands of power during outages; they could also provide local generation for utilities to restore from the distribution system outwards by connecting such small islands, as opposed to bringing power in from the bulk power system. While it may be possible to configure such resources to speed the process of supplying power to some priority loads, that would also unburden the primary black-start restoration process. At high levels of penetration, there may be an opportunity to factor DERs into black-start restoration plans. For example, multiple islands in the system formed by microgrids could be connected to form larger islands. Doing that might give the utilities more assets and more flexibility in their black-start planning.

**Finding:** The presence of a significant amount of DERs could provide a limited amount of local power during outages and could also be factored into black-start and



emergency planning if appropriate system upgrades have been made and utility operators have visibility into their operating status and controllability of their performance.

**Recommendation 6.3:** The Department of Energy and utilities should evaluate the technical and contractual requirements for using distributed energy resources as part of restoration activities, even when these assets are not owned by the utility, to improve restoration and overall resilience. Emergency management and restoration plans should include the owners of distributed energy resource assets, including owners with generation, storage, or load-control capabilities.

### Monitoring and Control

The monitoring and control of the power grid is accomplished through the supervisory control and data acquisition (SCADA) system and other supporting technologies, as described in previous chapters. At the control center, software tools aggregate diverse data to provide situational awareness and support operator decision making (e.g., energy management systems [EMS] on the transmission system and distribution management systems [DMS] on the distribution side). These systems gather measurement data from sensors deployed throughout the transmission and distribution systems and send out control signals. Additional sensor technologies exist for monitoring the health of circuits and components during and after restoration, which can confirm to repair crews that damage has been corrected; however, to the committee's knowledge, these have not been licensed or developed as commercial products. SCADA systems utilize robust, low-latency communications and are extremely helpful in assessing the state of damage to the system and identifying the centralized and distributed resources available for restoration. The communication networks enabling this monitoring and control are often dedicated infrastructure under the direct jurisdiction of the operating entity but are sometimes leased or provisioned by third parties.

DERs could also be monitored and controlled using the same SCADA system, in which case it would be easier for the DER to assist with restoration activities. If the DER is dispatched through a different monitoring and control communications infrastructure, it may be more difficult to provide restoration services due to the complications of coordinating among different systems. After a major disturbance, the status of the DERs, as well as the rest of the grid components, can only be known if the sensors and communication networks are not damaged or shut down by the disturbance. Electric power operators must restore power control systems and supporting communications systems concurrently with, and as an integral part of, grid restoration. Restoration of control systems and their associated communications infrastructure must remain an integral part of resilience planning.

### Recovery Depends on the Type of Damage

Beyond the generalized description of the recovery process, the details of restoration activities can be very different for different types of events and resulting damage. For example, a cascading blackout can cause a large area to lose power, but recovery may be relatively rapid and straightforward if no significant physical damage has been done to system components. Likewise, restoration—and specifically damage assessment—is considerably easier when the grid's cyber monitoring and control systems are intact and operational, compared to a potential cyber attack that diminishes a utility's situational awareness. In contrast, a strong, slow-moving hurricane can cause destruction and flooding over hundreds of square miles of coastal community, making post-event access very difficult. The following sections describe opportunities to improve recovery to outages with different types of damage, as categorized in Figure 3.2.

### DISRUPTIONS THAT INVOLVE ACROSS-THE-BOARD DAMAGE TO THE GRID AND ITS SUPPORTING INFRASTRUCTURE

Perhaps the most difficult disruptions to recover from are those that simultaneously cause damage to the physical components of the electricity system, the cyber monitoring and control systems, and critical supporting infrastructure. Damages of this sort can result from major natural disasters such as hurricanes and tropical storms, floods, winter storms, and earthquakes. Table 6A.1 provides details for each of these hazards in terms of the six stages of the outage life cycle—plan, prepare, event, assess, restore, and recover. Table 6A.2 lists two additional events, tornado and geomagnetic disturbances (space weather), that can also cause widespread damage.

While all of these events involve physical damage to the power system, there can be considerable variation in the extent of damage to other supporting infrastructures and the community. For example, damage from a major hurricane is typically widespread, inflicted on transportation and other critical infrastructures, and can greatly diminish local electricity consumption. In contrast, as Table 6A.1 notes, the spatial extent of damage from flooding depends significantly on local topology: in some cases much of the community may be unaffected, whereas communities and infrastructure in flat and low-lying terrains may be entirely destroyed. Clearly these two situations result in dramatically different restoration environments. Restoring a system from nearby dry ground that has all facilities intact and working is far easier than operating in an environment where everything for miles around has been submerged. Utilities generally know what sort of circumstance they will face in the event of a disaster and plan accordingly.

In some situations, there is sufficient warning time to assess whether critical system components will be at risk and, when possible, take preventative actions. While utilities

strive to maintain electrical service at all times, sometimes taking steps that will speed recovery after an inevitable outage should take precedence over keeping power on as long as possible before an outage. For example, a utility will know which substations are exposed to high flood risk and may preemptively power down certain parts of the system to prevent more substantial damage from flooding energized facilities. There are circumstances in which de-energizing vulnerable components *before* an event occurs could better protect them from damage and make recovery much faster.

**Recommendation 6.4:** Electric service providers should identify those components and corresponding events for which pre-event de-energizing of selected assets is the lowest risk strategy and develop regulatory, communication (especially with customers), and other plans that allow such protective action to be implemented.

### Assessing System Damage

As Figure 6.1 notes, the first step in restoration is to assess the state of the system. Where the monitoring and control system is still operating, it can be used to perform a rapid assessment. More monitoring and control is available at the transmission level, but SCADA at the distribution level is also being deployed, driven in part by the increase in DERs and other advanced technologies. This monitoring is also extending to the customer level with advanced metering infrastructure (AMI) and distribution technologies. Rather than depending on customer phone calls, some outage management systems (OMSs) receive direct telemetry from AMI and other sensors to develop a comprehensive view of customer outages.

Where the communications network supporting the SCADA system or other measurement telemetry is damaged, the traditional strategy is to send crews out to do on-site inspections. At the transmission level, aircraft are often used to locate downed lines, towers, and other damage. Normally aircraft would be operating directly under the jurisdiction of the electricity utility operator, as their assets are also used for routine right-of-way patrols. If necessary, electricity operators are able to acquire additional aircraft through leasing or other arrangements. During large national-level events, other government agencies can provide aerial surveillance capabilities if they are not directly involved in search and rescue operations. The Civil Air Patrol,<sup>1</sup> a civilian auxiliary

of the U.S. Air Force, has also been leveraged to provide aerial photographic sorties following disasters.

A new option coming into serious consideration is the use of unmanned aerial vehicles (UAVs), commonly known as drones (Olearczyk, 2013; Miller et al., 2014). Such vehicles can systematically survey damage to a system using both visible light and infrared imagery. Some UAVs have a fixed-wing design, but others are more maneuverable and can hover over problem areas for a long duration. The results of UAV inspections will be most useful if a utility has previously built a geocoded baseline of its entire system. This allows new imagery to be compared with baseline imagery and combined with asset management tools and workforce management systems to establish and coordinate repair priorities and progress (Miller et al., 2014).

The operation of UAVs in the United States is under the jurisdiction of the Federal Aviation Administration (FAA), which has been adopting new rules governing the commercial application of UAVs. However, these regulations have not kept pace with the rapid technological advancement of these systems, and there remains uncertainty surrounding the viability of UAVs for this application. In July 2016, Congress passed the FAA Extension, Safety, and Security Act of 2016.<sup>2</sup> Section 2207 of that law requires FAA, no later than 90 days after enactment, to “publish guidance for application for, and procedures for the processing of, on an emergency basis, exemptions or certificates of authorization or waiver for the use of unmanned aerial systems by civil or public operators in response to a catastrophe, disaster, or other emergency to facilitate emergency response operations, such as firefighting, search and rescue and utility and infrastructure restoration efforts.” As of this writing, that guidance has not yet been issued. A system that relies on temporary FAA authorization creates barriers to adopting this technology for electricity service restoration, since the capability to use UAVs for damage assessment needs to be developed, exercised, and refined in advance of a disaster rather than cultivated during the incident.

A continuing problem with the use of UAVs, both for post-disaster assessment as well as for routine surveillance and maintenance of transmission and distribution systems, has been the FAA restriction that such vehicles can only be used within the UAV pilot’s line of sight. In the event of a large-scale disaster, such a restriction seriously limits how useful UAVs can be. Several utilities have been experimenting with the use of UAVs and have obtained FAA 333 permits.<sup>3</sup> Some limited use of UAVs for post-disaster surveillance has also

<sup>1</sup> The Civil Air Patrol (CAP) is a congressionally chartered, federally supported non-profit corporation that serves as the official civilian auxiliary of the U.S. Air Force. CAP is a volunteer organization that performs three congressionally assigned key missions: emergency services (e.g., search and rescue and disaster relief operations), aerospace education for youth and the general public, and cadet programs for teenage youth. In addition, CAP has recently been tasked with homeland security and courier service missions. CAP also performs non-auxiliary missions for various governmental and private agencies, such as local law enforcement and the American Red Cross.

<sup>2</sup> Public Law No. 114-190 (2016).

<sup>3</sup> FAA Section 333 “grants the Secretary of Transportation the authority to determine whether an airworthiness certificate is required for a unmanned aircraft system to operate safely in the National Airspace System.” As of 2015, the number of FAA 333 exemption permits granted to Duke was 16; San Diego Gas & Electric was 8; Pacific Gas & Electric was 5; Southern Company was 4; and NextEra Energy was 4.

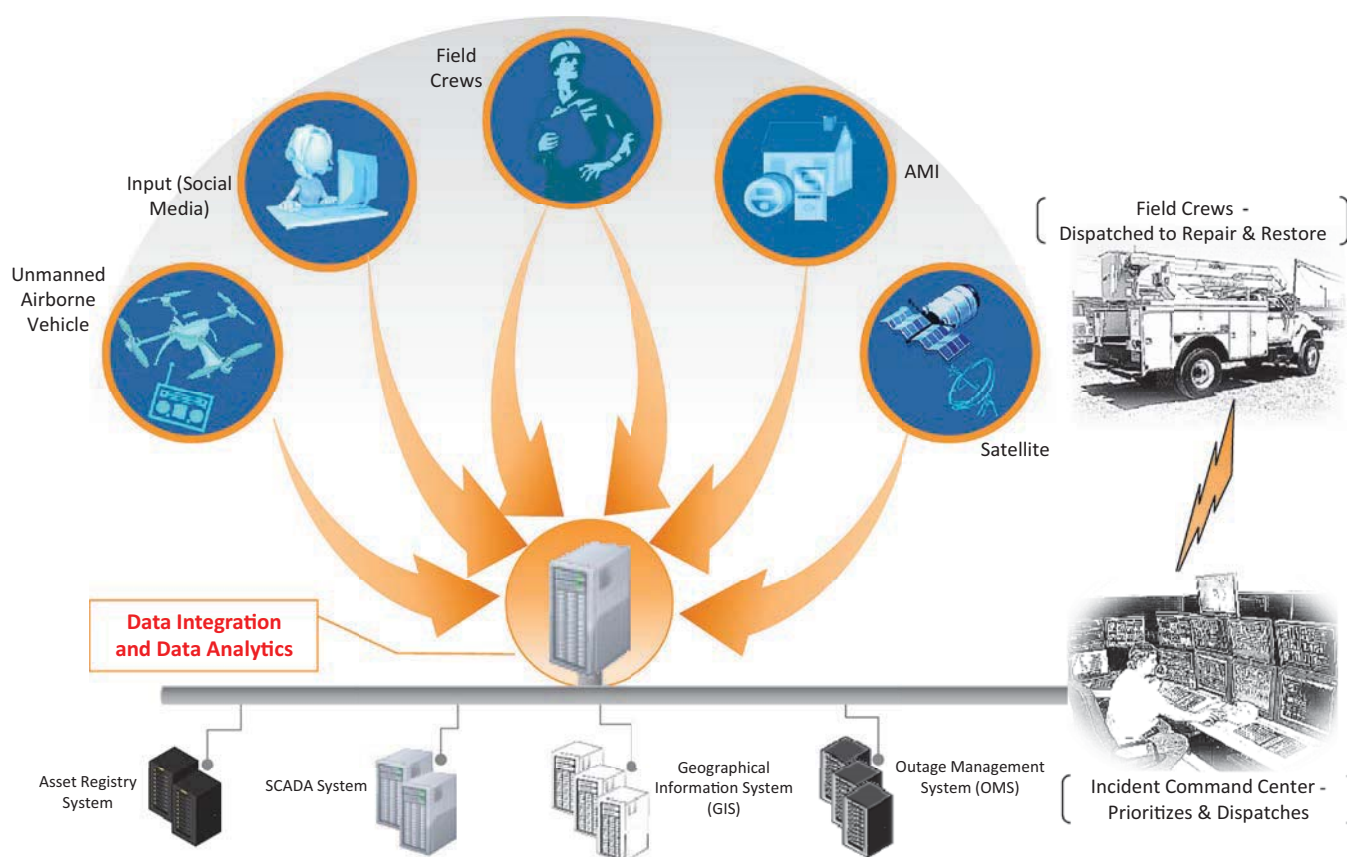


occurred under FAA Part 107 waivers following Hurricane Matthew, which aided in damage assessment and expedited recovery. However, both Section 333 and Part 107 permits require pilots to maintain line-of-sight operations, and any operation beyond line of sight requires additional FAA authorization. At the time of this writing, very few waivers for granting operation beyond line of sight have been granted, and these have been primarily to specialized testing and research organizations. While FAA can grant exceptions on an ad hoc basis, this takes time. It would be far better to have standing arrangements for the use of drones in emergency situations.

**Recommendation 6.5:** With convening support by the Department of Energy, the electricity industry should proactively engage the Federal Aviation Administration to ensure that the rules regulating unmanned aerial vehicle operation support the rapid, safe, and effective applications of unmanned aerial vehicle technology in electricity restoration activities, including pre-disaster tests and drills.

### Data Fusion to Enhance Restoration Activities

In addition to the OMS that tracks customer outages and correlates these data with geospatial feeder data to determine where repair crews should be sent, other available data from various sources such as weather forecasts and news reports are being used to aid restoration activities (Figure 6.2). An area for research is the use of additional, underutilized information such as social media—Internet resources and social media are widely used to distribute information to consumers during a disaster. It is also possible to make use of information from consumers; however, systems are not generally in place to accomplish this. For example, during and immediately after Superstorm Sandy, many individuals sent images of downed lines, trees, and damaged equipment to utilities. If this information were automatically geotagged and time stamped, it could have provided valuable information to aid in restoration activities. Unfortunately, at the time, utilities struggled to make use of the information as it arrived in high volumes over non-traditional channels. Additionally, there was a need to ensure that public messaging was consistent,



**FIGURE 6.2** Example of data integration to support advanced data analytics for improved restoration efforts. The image above is not comprehensive and other technologies—for example, real-time asset health monitoring equipment and manned airborne vehicles—can be used to collect and relay information on the health of transmission and distribution system components.

NOTE: AMI, advanced metering infrastructure.

SOURCE: EPRI (2013).

such as continuing to advise the public never to approach downed electrical equipment.

### Access to Replacement Parts, Particularly Large Transformers

While line crews are able to repair downed power lines, towers, and poles, and repair or replace low- and medium-voltage distribution transformers, damage to large substation equipment can be much more problematic. These substations contain high-voltage transformers, circuit breakers, and other large equipment that, if damaged, can be difficult and expensive to replace. Extra-high-voltage transformers (i.e., 345 kV and above) are especially problematic. These are large devices that are expensive, have long manufacturing lead times, and are hard to move. In many cases, the electrical properties of high-voltage transformers have been customized to fit the specific locations in which they are installed. It has long been understood that these transformers are an especially vulnerable element of the grid (OTA, 1990; NRC, 2012; DOE, 2015; Parfomak, 2014). While spare transformers can become a major issue in outage events that cause broad physical damage, they are especially important in the context of terrorist events where they could become the focal target of intentional attack. Indeed, as far back as 1990, the Office of Technology Assessment concluded that, if a terrorist group wanted to attack the U.S. power system, the obvious target would be a carefully selected set of high-voltage power transformers. *Terrorism and the Electric Power Delivery System* explained the following:

The large power transformers in generating station switch yards and major substations are vulnerable to terrorist attack

and could take months or years to replace. Options for bypassing damaged substations to bring power from remote generating stations to load centers are very limited because the grid is already stressed during peak demand. The result of a coordinated attack on key substations could be rolling blackouts over a wide area until the substations are repaired. Under such conditions, the availability of compact easily transported recovery transformers would be invaluable (NRC, 2012).

The report went on to recommend that the Department of Homeland Security (DHS) cooperate with DOE to “complete the development and demonstration of high-voltage recovery transformers and develop plans for manufacturer storage and installation of these recovery transformers” (NRC, 2012). In a demonstration program called RecX (for “recovery transformer”), the DHS Science and Technology Directorate teamed with ABB and the power industry to manufacture three single-phase 345 kV transformers in St. Louis, Missouri, and move them to Houston, Texas, in March 2013 (Figure 6.3), where they were installed and operated in a substation. The entire move and installation was completed in less than 1 week (DHS, 2014).

Regulators, policy makers, and utilities recognize the need to stockpile spare equipment, especially large equipment that can be difficult and expensive to replace. As summarized in a recent Congressional Research Service report (Parfomak, 2014), the industry has made some progress in constructing a catalogue of spare high-voltage transformers. DOE recently released a request for information to gather input on setting up a national transformer reserve, and eight private energy companies have launched Grid Assurance,<sup>TM</sup> an independent company that will stockpile transformers



**FIGURE 6.3** Three ABB single-phase 345 kV compact replacement transformers being moved from St. Louis, Missouri, to a substation in Houston, Texas, under a Department of Homeland Security demonstration project.  
SOURCE: DHS (2012).

and other critical equipment.<sup>4</sup> A central issue with respect to developing a stockpile of replacement transformers is how to cover the cost. The approach taken by Grid Assurance,<sup>TM</sup> in which participating utilities have helped finance the founding of the company, and in return the company will sell stockpiled equipment to participating utility companies who need them during emergencies, was recently given a boost when FERC allowed participating utilities to recover their costs associated with purchasing sparing service and spare equipment.

Given the inherent challenge to knowing in advance where the need might arise to replace multiple transformers, some argue that building a modest stockpile is a collective national asset that should be covered, or at least partly subsidized, with federal tax dollars. Congress is contemplating the creation of a national strategic transformer reserve (DOE, 2017). However, if federal resources are invested in building such a stockpile, clear policy must be developed to limit its use to well-specified disaster scenarios. Without such policy, there is a risk that industry could become overly reliant on the stockpiled equipment and reduce investment in its own spare equipment stockpiles and programs. Such an outcome could result in negligible net improvement of spare equipment capability for the nation, rather than just shifting from industry-purchased stockpiles to government-purchased stockpiles.

In its 2015 Quadrennial Energy Review (QER), DOE noted that “the use of smaller, less-efficient, temporary replacement transformers may be appropriate for emergency circumstances. In 2006, [EPRI] suggested building compact ‘restoration transformers’ that would fit on large cargo aircraft and trucks. Since then, DHS’s Recovery Transformer Program has developed and tested a flexible transformer that is transportable by truck [see Figure 6.3] and can be installed within several days of an incident. These technologies could help address logistical concerns with moving large transformers in the event of disruptions” (DOE, 2015). The QER concluded that high-voltage transformers “represent one of [the grid’s] most vulnerable components. Despite expanded efforts by industry and federal regulators, current programs to address the vulnerability may not be adequate to address the security and reliability concerns associated with simultaneous failures of multiple high-voltage transformers” (DOE, 2015). The 2017 QER also discusses this issue, noting the following:

There are currently three key industry-led, transformer-sharing programs in the United States—NERC’s Spare Equipment Database program, Edison Electric Institute’s Spare Transformer Equipment Program, and SpareConnect. Another program, Recovery Transformer, developed a rapidly deployable prototype transformer designed to replace the most common high-voltage transformers, which

DHS successfully funded in partnership with Electric Power Research Institute and completed in 2014. . . . As of December 2016, three additional programs—Grid Assurance, Wattstock, and Regional Equipment Sharing for Transmission Outage Restoration (commonly referred to as RESTORE)—are in development. . . . In December 2015, Congress directed DOE to develop a plan to establish a strategic transformer reserve in consultation with various industry stakeholders in the FAST Act. To assess plan options, DOE commissioned Oak Ridge National Laboratory to perform a technical analysis that would provide data necessary to evaluate the need for and feasibility of a strategic transformer reserve. The objective of the study was to determine if, after a severe event, extensive damage to [large power transformers] and lack of adequate replacement LPTs would render the grid dysfunctional for an extended period (several months to years) until replacement LPTs could be manufactured. DOE’s recommendations will be published in the report to Congress in early 2017 (DOE, 2017).

Over the next two decades, the grid will see increasing use of solid-state transformers and other solid-state power electronics, though penetration at present is nascent. The durability and resilience of this technology will have to be established over time and restoration plans adjusted accordingly. Solid-state power electronics will offer greater operational flexibility than traditional technology, which may be useful when the grid is being operated in non-standard ways. This technology will likely see its first widespread use in lower-power distribution systems. Recently, DOE has been supporting the development of advanced designs for LPTs. Specifically, they have been working to do the following:

Stimulate innovative designs that promote greater standardization (i.e., commoditize LPTs) to increase grid resilience (i.e., faster recovery) in the event of the loss of one or more LPTs. To this end, new designs must maintain high efficiencies, have variable impedances, accommodate various high-side and low-side voltages, and be cost-effective compared to traditional LPTs. Projects would be expected to involve modeling, analyses, and exploratory research to assess the performance and economics of proposed designs (DOE, 2016). A critical value of [this] research, beyond the development of advanced designs, is increased standardization of components improving agile allocation during disasters (DOE, 2016).

The committee recommends a dual strategy: On the one hand, the nation should push forward to improving the availability of conventional and replacement transformers for use in the event of physical disruption. At the same time, DOE should continue to explore advanced LPT designs that, in the longer term, could lower cost and improve the efficacy of emergency replacements. The vulnerability to grid operation posed by accidental or intentional damage to high-voltage transformers has been understood for decades. While limited progress has been made to reduce this vulnerability, it continues to pose a serious risk to the power system.

<sup>4</sup> Grid Assurance<sup>TM</sup> ([www.gridassurance.com](http://www.gridassurance.com)) was founded by affiliates of American Electric Power, Berkshire Hathaway Energy, Edison International, Eversource Energy, and Great Plains Energy.



**Recommendation 6.6:** The Department of Homeland Security, the Department of Energy, the U.S. Congress, and the power industry should be more aggressive in finding a way to address the issue of manufacturing and stockpiling flexible, high-voltage replacement transformers as an important component of infrastructure investment initiatives. If federal funds are used to help in doing this, policy will be needed to limit stockpile use to major disasters. Otherwise, utilities might face incentives to reduce their stockpiles for dealing with more routine events.

**Finding:** Development of innovative approaches for making LPTs with greater operational flexibility (e.g., variable impedances, accommodating multiple voltages) while maintaining high efficiency and cost effectiveness relative to traditional LPTs is promising. If such devices can be developed with standardized components, they could play an important role in expediting restoration of the grid when physical damage has occurred to LPTs.

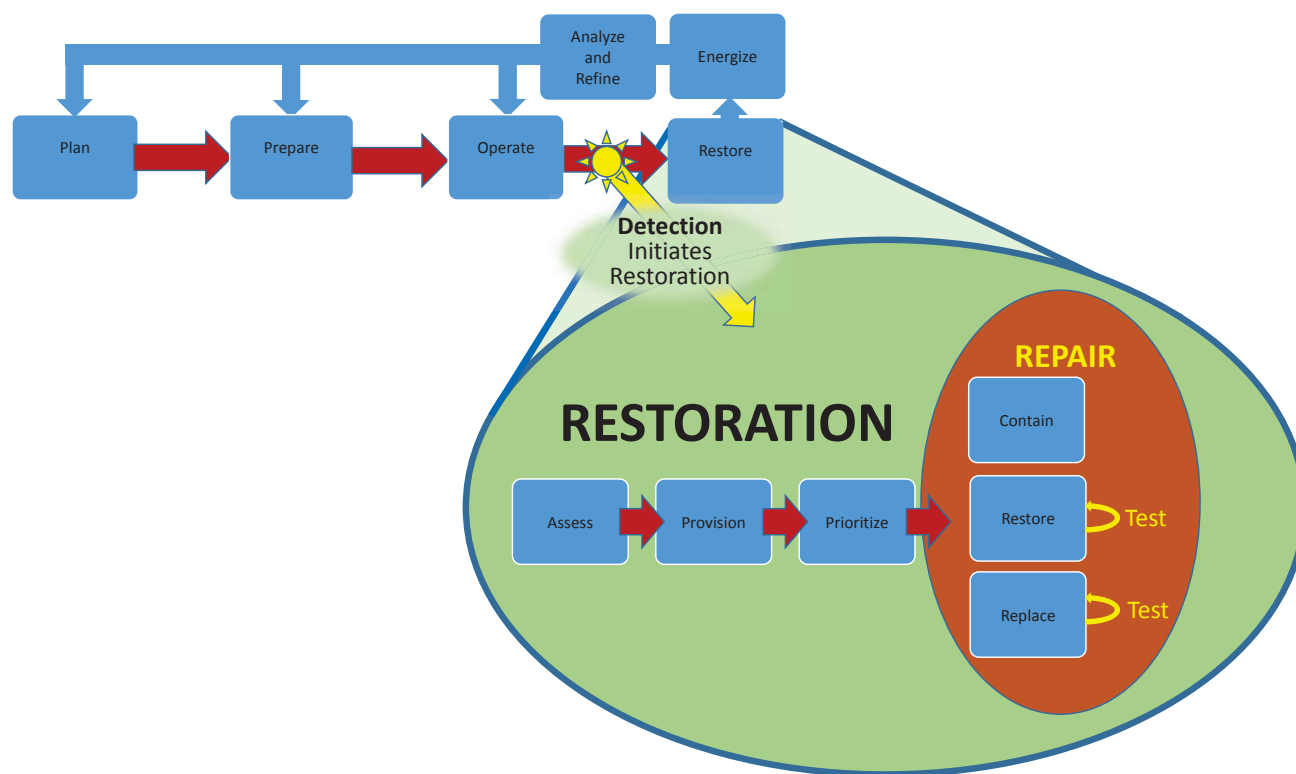
**Recommendation 6.7:** The Department of Energy should continue to support research and development of advanced large power transformers, concentrating on moving beyond design studies to conduct several demonstration projects.

## DISRUPTIONS THAT INVOLVE DAMAGE TO THE CYBER MONITORING AND CONTROL SYSTEMS

A second restoration case is recovery from damage to the cyber monitoring and control system as a result of a cyber attack that leads to a major service disruption. Restoration from such disruptions is structured around the process shown in Figure 6.4, which contextualizes active restoration within the larger process that begins with planning for cyber restoration in much the same way as utilities plan for physical restoration. Active cyber restoration begins with detecting a breach and follows the same sequence of activities introduced above: assess, provide, prioritize, and repair. This section focuses on the steps that occur to restore power after a cyber detection that has resulted in a major service disruption.

### Detect

One important difference between a cyber failure and a physical disaster is the tightly defined nature of the cyber attack. The impact of a hurricane is expressed in maps as well as in lists of damaged equipment and lines. In the case of a cyber event, the cause is usually more singular than that of a natural disaster. It would be a rare event that would involve the simultaneous breach by two disparate organizations in two different ways, although a well-prepared mal-actor



**FIGURE 6.4** Restoration of industrial control systems after a cyber breach.

may seek to create exactly this situation. The analysis of a cyber event typically focuses on understanding a specific bit of malware and how it affects communication, and the countermeasures are similarly focused and technical unless the impact extends to the point of requiring replacement of substantial equipment.

A breach of a utility industrial control system (ICS) can be obvious after the system it is controlling malfunctions, but this malfunction may not occur for a long time after the initial breach. For example, in the well-covered breach of the Ukrainian power system, the actual disruption occurred 9 months after the initial breach. Mandiant (2016) reported that the average time from breach to detection in a typical information technology system is 140 days. This time delay is important and pernicious as it allows attackers to locate and master critical systems, find valuable or restricted information, and develop a strategy for exploitation. Adversaries lacking detailed knowledge of a system do not know a priori how to inflict damage even if they have accessed the ICS; they need this time to learn how to damage the breached system. The first step in cyber restoration is to detect the breach quickly, so that the adversary does not have time to develop sufficient understanding of the ICS to disrupt operations. Utilities need to develop reliable mechanisms to verify that their systems are running only the expected software and, if this is not the case, to allow remote resetting of systems.

**Finding:** Breaches of utility industrial control systems may persist for an extended period prior to causing disruptions to operations or service. A breach alone is not sufficient to gain control of a system, to compromise its operation, or to steal or corrupt valuable information. It takes time for attackers to learn about the system they have breached.

The problem of breach detection can be addressed by anomaly detection, although this approach has not been shown to work as well in more general enterprise settings. In part, this is because complex and distributed systems of large enterprise systems are difficult to monitor, as the variety of communications is immense (e.g., from e-mail to web site configuration management and integration with multiple systems) and varies over time. However, electric utility ICS systems are different. The boundaries of the system are more clearly defined and slower to change, the network architecture is more consistent, the communications are more structured (i.e., using well-defined protocols), and the values communicated fall into definable ranges and patterns. For example, residential meters typically report every day, hour, or 15 minutes, depending on configuration; they always use a message structure defined by the brand of meter (frequently based on an open standard), and the voltages they report are almost always in the American National Standards Institute band.<sup>5</sup> Using another protocol,

reporting a value substantially outside the American National Standards Institute band, issuing a different message type, or reporting too often could indicate that the meter has been compromised or is malfunctioning. Another example of the potential for anomaly detection is reclosers, which control the connection to a lateral power line and do not open or close very often. Too-frequent cycling could indicate an attempt to damage the system.

Beyond these patterns, the electricity system is governed by the physics of its electrical flows. Information from the numerous and diverse sensors must present a coherent model of the state of the conditions on the grid. Reported values which deviate from the physically possible can indicate either a broken sensor or a cyber issue. For these reasons, anomaly detection methods that are not effective in general enterprise systems can work well in utility control systems. Anomalies can be detected based on rules derived by various means, including those that are (1) specified by operators, (2) derived from network mapping, (3) derived through machine learning, and (4) based on physical modeling. The first two of these are based on established technology (e.g., The Bro Project<sup>6</sup> and the Essence Project<sup>7</sup>). There is much potential for progress in the latter two. Machine learning could combine support vector machine estimation for classification with neural net methods for training. While good physics models are available (e.g., OpenDSS and GridLab-D for distribution systems), there are challenges in making them fast enough for use in real-time anomaly detection.

**Finding:** Tools for physics models and ICS network modeling are not well adapted to use in anomaly detection or cyber testing. Any discrepancy between the physics of the grid and the telemetry can indicate a system or component problem or a cyber compromise. The challenge at present is that physics models of power flow are generally too slow for real-time monitoring, and the track record for calibration is spotty.

**Recommendation 6.8:** The Department of Energy should develop the ability to apply physics-based modeling to anomaly detection. There is enormous value in having real-time or better physics models in deriving optimal power flow and monitoring performance for more accurate state estimation. Such systems should also provide a powerful tool for verifying the integrity of telemetry systems—that is, verifying that observed conditions are consistent with model conditions—and if not, then there is a problem with knowledge of state, presuming the model is accurate.

<sup>5</sup> American National Standards Institute Standard C84.1 defines the acceptable range of voltage within which a utility can deliver power to customers.

<sup>6</sup> The website for the Bro Project is <https://www.bro.org/>, accessed July 11, 2017.

<sup>7</sup> The website for the Essence Project is <https://www.controlsystemsroadmap.net/Efforts/Pages/Essence.aspx>, accessed July 11, 2017.

## Assess

Once a breach of the ICS has been detected, the next step is to assess the extent of damage. At this point, power may still be flowing to part or all of the grid; however, the system has failed fundamentally because the ability to determine system state accurately and control component behavior is likely compromised. Work should begin immediately to determine what part of the system (including the ICS, all connected components, and communications in either direction with external systems) has been compromised and how. At the simplest level, this involves examination of all components for indicators of compromise. Examination can include the following:

- *Inspection.* Scanning the memory and storage of each device looking for malware (i.e., “blacklisting”) and checking that only approved software is running (i.e., “whitelisting”).
- *Challenge.* Exercising devices to verify that they are communicating and operating correctly (e.g., flip a switch electronically to verify that it can be reached, acts as directed, and can confirm its action and state).
- *Diagnostic model.* Network and physics-based modeling of the grid to map anomalous behavior, although currently the models that would be used for this are not yet ready to support near-real-time restoration.

The first steps in assessment are to assemble the necessary tools if they are not present, make sure that the tools and their underlying databases are up-to-date, and then systematically and completely examine every software object in the broadly defined system to determine whether and how each has been corrupted. The assessment should be undertaken with a sense of the system connectedness, first emphasizing components that are linked to and dependent on systems known to be compromised, within the same security domain, or accessed in similar ways.

## Provide

The provisioning phase of restoration focuses on marshalling human and other resources necessary to bring the ICS back to operation, perhaps in stages. Based on the assessment, the restoration team derives a list of skills and artifacts necessary to restore each component and the integrated system. In instances where replacement is either necessary or more efficient, these lists will include hardware (e.g., servers, smart components). For example, if a server is corrupted, it may be possible to restore it to safe operation, but it may be quicker and easier to build a new server from scratch and return the original server to inventory at a less hectic time. Restoration may also require software and data: reference disks of software, often termed “gold disks,” are typically required, as are backups of the most current

state data. Large transmission organizations are generally scrupulous about maintaining “gold disks,” but this practice has not been promulgated throughout the entire industry. Restoration can be slowed by something as simple as not having license information, not patching backups to current levels, or not having internet access when it is required for activation or download of current patches. The provisioning plan should take all of these activities into consideration. The provisioning plan, overlaid on the assessment, provides a map of what components and subsystems can be restored and with what effort.

## Prioritize

Based on the assessment, a plan must be developed to restore the system. The challenge is to coordinate the activities of specialists with the available physical and digital resources in a sequence of steps. Restoration of a specific computer could range from something as simple as running a virus removal tool to something as complex as writing new code for a virus removal tool. It could involve re-flashing a build image, replacing a drive or even a whole computer, or rebuilding a software configuration step-by-step. There may be hundreds of steps, and it may be impossible to determine in detail all of the steps needed in a particular case. Initially, the plan may state only that a network engineer will look at an infected switch and determine what needs to be done to repair it. As the restoration proceeds, knowledge of state and the efficacy of restoration options improve, and the plan becomes more specific.

A critical issue is the affected utility’s ability to marshal appropriately skilled resources. The design and documentation of utility ICS systems is insufficiently standardized; outside experts cannot quickly become effective in another organization. They can be tasked with routine tasks like imaging a disk, but their ability to contribute more strategically requires more detailed knowledge of affected systems. Priorities to achieve cyber resilience include establishing a common design and technical lexicon, training and working across organizations, and establishing common practices and formats for supporting artifacts. These need not be accomplished across the nation in a single push; rather, they can develop in groups of related or associated organizations, such as the group of distribution cooperatives supported by the single generation and transmission cooperative North Carolina Electric Membership Corporation. This model should be broadened to include other peer groups, perhaps organized around regional transmission organizations and regional reliability coordinators.

Another major barrier is that, to date, organizations have not been transparent about cyber events, in part owing to risk of embarrassment and liability. Furthermore, mechanisms to share resources for cyber restoration and compensate for their use—that is, cyber mutual assistance agreements analogous to traditional MAAs—are nascent. Working with



EEI, the Electricity Subsector Coordinating Council is developing such a cyber MAA program (ESCC, 2016); however, the configuration of local systems can differ so substantially across utilities (i.e., when comparing a small cooperative to a major independent system operator/regional transmission organization) that it may be prohibitively difficult for loaned workers to contribute significantly to cyber restoration, even if they are experts. Through a separate program, the Electricity Information Sharing and Analysis Center (E-ISAC) disseminates risk information to utilities; its further development should be encouraged, but the emphasis to date has been on sharing information rather than labor and primarily directed at protection rather than restoration.

One final issue to consider is funding; cyber restoration, like physical restoration, can be costly. Means must be made available for utilities to hire outside assistance when useful and buy new equipment as needed to restore power quickly. A utility may look at its limited resources and plan restoration over a long period, but there may be a social advantage to using resources beyond the utility to restore over a shorter period.

**Finding:** To date, there have been no large-scale power outages in the United States caused by cyber attacks, but there have been many instances in which components have been compromised. Utilities have experience in fixing these minor cyber problems by rebuilding components and databases. However, cyber restoration is not a routinized process, and different organizations follow different approaches based on the nature of the event.

**Recommendation 6.9:** The Department of Energy and the Department of Homeland Security should work with the North American Electric Reliability Corporation, independent system operators, and regional transmission organizations to develop a model for large-scale cyber restoration. This should be done in collaboration with utilities and leading utility organizations such as the Edison Electric Institute, the National Rural Electric Cooperative Association, the Electric Power Research Institute, and the American Public Power Association.

## Repair

Actual repairs are accomplished in three steps: (1) containing the breach, (2) restoring components that can be saved, and (3) replacing those that cannot.

## Contain

The first step after detection is to contain the malware by isolating it and preventing its spread to other internal or external systems. Taking an infected component off-line can adversely impact grid operations; thus, expert decisions must be made about how to operate without the impacted

components. Operations without compromised or degraded digital control may be possible; if not, a portion of the grid may be operated instead. For example, if the problem impacts voltage control at a particular substation, the feeder may be disconnected from central control and either operated with fixed typical control points or shut down temporarily. In this case, potentially no service will be lost. It is critical to keep safety and the long-term reliability of the grid in mind; operation should not be attempted unless it can be verified that the grid and customers are not put at risk. If digital telemetry is lacking, this may require dispatch of crews to verify switch settings manually, determine voltage and current, or confirm whether a line is energized. Fortunately, protective relays and fuses provide some protection against egregious misoperation.

Another aspect of containment is to communicate with other utilities. Sharing details of the attack—particularly information on the types of components impacted, the IP addresses of the attackers if known, and any identified malware signatures—may help others identify an ongoing attack. The E-ISAC has taken on the role of intermediary in this action; nonetheless, these systems must be strengthened, extended, accelerated, and exercised. The Cybersecurity Risk Information Sharing Program, initiated by DOE with E-ISAC support, is currently monitoring the majority of transmission systems and sharing such information with automated machine-to-machine communication. This has led to substantial improvement in the situational awareness of real-time cybersecurity risks in the electricity industry.

## Restore and Replace

With the spread of malware contained to the extent possible, the work shifts to restoring components to a clean state or replacing them if repair is too difficult or time consuming. As practice in cyber restoration moves beyond improvisation, restoration will eventually proceed by following a plan that is developed in advance, updated, and refined for specific circumstances. Implementing the plan requires the following: (1) Executing the outlined steps, (2) Adding detail as necessary and possible, (3) Testing, (4) Monitoring progress and failure, and (5) Providing feedback to update the plan.

At each point in the restoration, the engineer must determine the correct strategy: restore or replace. The trade-offs include cost, time, and the relative risk of a repaired component still hiding malware or being otherwise compromised versus possible errors in the configuration of new components. The choice is specific to the circumstances at hand. For example, the time required for repairs depends critically on whether there is a tested and trusted tool available on hand to remove malware and whether complete and correct backup data are available.

Highly competent staff are key to effective execution of restoration and replacement plans. While a utility may

have excellent general support staff, it is unlikely that they will have experience in large-scale cyber restoration. Their skills, experience, and confidence must allow them to innovate and improvise beyond their current skills. Government teams experienced in cyber restoration and similarly skilled staff from other utilities, software vendors, and cybersecurity firms can provide valuable support to the utility teams, although they are still limited by their lack of experience with the particular system being restored.

**Finding:** There has been a tendency among utilities and other commercial entities not to share information about cyber breaches and to look inward rather than seeking help, which limits potential for collaboration across organizations. Most utilities are not likely to have adequate internal staff directly experienced in large-scale cyber restoration. Furthermore, the ability of outside entities to help a utility with cyber restoration is limited by unfamiliarity with the configuration of the impacted system and by the lack of agreed-upon standards or shared practices. The ICS architecture at one utility may have little in common with the ICS at another utility, independent of the physical differences in the electrical system. This lack of commonality in utility ICS system designs and documentation makes rapid and efficient use of staff from other organizations very challenging, as an engineer at one utility may face a steep learning curve at another utility.

**Recommendation 6.10:** The Department of Energy and the Department of Homeland Security should work with the Electricity Subsector Coordinating Council and utilities to enhance the sharing of cyber restoration resources (i.e., cyber mutual assistance agreements) including personnel, focusing on peer-to-peer collaboration, as well as engagement with government, industry organizations, and commercial cybersecurity companies. Practices that allow shared personnel to more quickly come up to speed on restoration plans will increase the value of cyber mutual assistance agreements. This should include dissemination of best practices for the backup of utility industrial control systems and operational data.

**Finding:** Though the basic systems are in place for sharing cyber threat information, practices can be improved with more emphasis on speed. There are organizational systems in place for sharing cyber information (e.g., E-ISAC), but the lack of a common ontology and design patterns make the shared information more difficult than necessary to put to use.

**Recommendation 6.11:** The Department of Energy, the Department of Homeland Security, the electricity sector, and representatives of other key affected industries and sectors should continue to strengthen the bidirectional communication between federal cybersecurity programs and commercial software companies.

Effective documentation strategies are also critical for effective cyber restoration. System documentation must be complete, accurate, and up-to-date so that the restoration teams have the information they need to proceed and additional staff can be brought up to speed quickly. Industry experience has shown that the only way to keep documentation up-to-date is to connect it to operational production systems. For example, the network should be mapped periodically and continuously using automated tools, and then the discovered reality can be compared to the documented theory. Documentation should include backup copies of every critical system, including the data and software and all critical keys, passwords, and licenses. Such backup information should be available through a secure system with an expert in the loop.

Finally, cyber restoration workers need the best possible tools to facilitate their collaboration. At a minimum, telephones should be supplemented with shared drives, online screen sharing, and remote disk access. Cloud options should be available to provide backup if local systems are compromised to the extent possible and vice versa. Such cloud systems must be as secure as possible and potentially open only to utility operators. Furthermore, these teams must practice with either real systems or high-fidelity models. (It is possible to construct virtual systems that would allow training and practice.) Strategies for this sort of simulator are being pursued by DOE, with the National Renewable Energy Laboratory in the lead, and by the National Rural Electric Cooperative Association, with its Simba project.

## Energize

Restoration of the ICS culminates with energizing the grid, shown at the top of Figure 6.4. There needs to be rapid iteration and tight integration between the plan and test steps, but ultimately the real-world test in the grid cannot be achieved digitally and virtually. Utility ICSs have switches and other controls that set machines in motion and power flowing. Some of these actions can be dangerous to line crews and could cause damage to utility and customer equipment as well as to other infrastructures. Also, a compromised control system may incorrectly alter limits on a fault protection relay or send signals to a generator that crews on site in the plant know are incorrect, resulting in dangerous system operations.

The scale and importance of utility operations dictate validation in many aspects of cyber restoration. The physics of the grid must be considered in all cyber decisions. Expert judgment is needed to determine when physical contact and observation are needed and when the benefits outweigh the risks. The training of utility personnel ensures a culture of safety.

## Analyze and Refine

After the grid is re-energized, the final step is to examine what was accomplished and gather lessons learned. The goal

**TABLE 6.1** Summary of Selected Recommendations Made by the National Research Council in Its 2012 Report *Terrorism and the Electric Power Delivery System*, Together with the Committee's Assessment of Where Things Now Stand

National Research Council Recommendation	Assessment of Present Situation
<p><b>6.1:</b> The Electric Reliability Organization (ERO) [NERC] should require power companies to re-examine their critical substations to identify service vulnerabilities to terrorist attack. Where such vulnerabilities are discovered, physical and cyber protection should be applied. In addition, the design of these substations should be modified with the goal of making them more flexible to allow for efficient reconfiguration in the event of a malicious attack on the power system. The bus configurations in these substations could have a significant impact on maintaining reliability in the event of a malicious attack on the power system. Bus layout or configuration could be a significant factor if a transformer, circuit breaker, instrument transformer, or bus work is blown up, possibly damaging nearby equipment.</p>	<p>The industry has made progress on this issue.</p>
<p><b>6.2:</b> The ERO and FERC should direct greater attention to vulnerability to multiple outages (e.g., n-2) planned by an intelligent adversary. In cases where major long-term outages are possible, reinforcements should be considered as long as costs are commensurate with the reduction of vulnerability and other possible benefits.</p>	<p>Some progress has been made on these issues, but additional effort is warranted.</p>
<p><b>7.6:</b> State legislatures should change utility law to explicitly allow microgrids with distributed generation. [Institute of Electrical and Electronics Engineers] should revise its standards to include the appropriate use of islanded distributed generation and microgrid resources for local islanding in emergency recovery operations. Utilities should re-examine and, if necessary, revise their distribution automation plans and capabilities in light of the possible need to selectively serve critical loads during extended restoration efforts. Public utility commissions should consider the potential emergency restoration benefits of distribution automation when they review utility applications involving such investments.</p>	<p>There has been some progress on this. Some states are considering whether and, if so, how to support the development of microgrids as well as the role of the local distribution utilities and other entities in the process of developing such systems. But additional effort is warranted.</p>
<p><b>8.1:</b> The Department of Homeland security and/or the Department of Energy should initiate and fund several model demonstration assessments each at the level of cities, counties, and states. These assessments should examine systematically the region's vulnerability to extended power outages and develop cost-effective strategies that can be adopted to reduce or, over time, eliminate such vulnerabilities. These model assessments should involve all relevant public and private participants including public and private parties providing law-enforcement: water, gas, sewage, healthcare, communications, transportation, fuel supply, banking, and food supply. These assessments should include a consideration of outages of long duration (<math>\geq</math> several weeks) and large geographic extent (over several states) since such outages could require a response different from those needed to deal with a shorter duration events (hours to a few days).</p>	<p>To the best of the committee's knowledge, no such demonstrations have been undertaken.</p>
<p><b>8.2:</b> Building on the results of these model assessments, DHS should develop, test, and disseminate guidelines and tools to assist cities, counties, states, and regions to conduct their own assessments and develop plans to reduce their vulnerabilities to extended power outages. DHS should also develop guidance for individuals to help them understand steps they can take to better prepare for and reduce their vulnerability in the event of extended blackouts.</p>	<p>To the best of the committee's knowledge, no such activity has been undertaken.</p>
<p><b>8.3:</b> State and local regions should use the tools provided by DHS as discussed in Recommendation 8.2 to undertake assessments of regional and local vulnerability to long-term outages, develop plans to collaboratively implement key strategies to reduce vulnerability, and assist private sector parties and individuals to identify steps they can take to reduce their vulnerabilities.</p>	<p>While not following the strategy that the committee recommended, some limited progress has been made.</p>
<p><b>8.4, 8.5, and 8.6:</b> Congress, DHS, and the states should provide resources and incentives to cover incremental costs associated with private and public sector risk prevention and mitigation efforts to reduce the societal impact of an extended grid outage. Such incentives could include incremental funding for those aspects of systems that provide a public good but little private benefit, R&amp;D support for new and emerging technology that will enhance the resiliency and restoration of the grid, and the development and implementation of building codes or ordinances that require alternate or backup sources of electric power for key facilities. . . . Federal and state agencies should identify legal barriers to data access, communications, and collaborative planning that could impede appropriate regional and local assessment and contingency planning for handling long-term outages. Political leaders of the jurisdictions involved should analyze the data security and privacy protection laws of their agencies with an eye to easing obstacles to collective planning and to facilitating smooth communication in a national or more localized emergency. . . . DHS should perform, or assist other federal agencies to perform, additional systematic assessment of the vulnerability of national infrastructure such as telecommunications and air traffic control in the face of extended and widespread loss of electric power, and then develop and implement strategies to reduce or eliminate vulnerabilities. Part of this work should include an assessment of the available surge capacity for large mobile generation sources. Such an assessment should include an examination of the feasibility of utilizing alternative sources of temporary power generation to meet emergency generation requirements (as identified by state, territorial, and local governments, the private sector, and nongovernmental organizations) in the event of a large-scale power outage of long duration. Such assessment should also include an examination of equipment availability, sources of power generation (mobile truck-mounted generators, naval and commercial ships, power barges, locomotives, and so on), transportation logistics, and system interconnection. When areas of potential shortages have been identified, plans should be developed and implemented to take corrective action and develop needed resource inventories, stockpiles, and mobilization plans.</p>	<p>Limited progress has been made on selected items.</p>

National Research Council Recommendation	Assessment of Present Situation
<p><b>9.1:</b> Complete the development and demonstration of high-voltage recovery transformers and develop plans for the manufacture storage and installation of these recovery transformers.</p> <p><b>9.2–9.6:</b> Continue the development and demonstration of the advanced computational system currently funded by the Department of Homeland Security and underway at the Electric Power Research Institute. This system is intended to assist in supporting more rapid estimation of the state of the system and broader system analysis. . . . Develop a visualization system for transmission control centers which will support informed operator decision making and reduce vulnerability to human errors. R&amp;D to this end is underway at the Electric Power Research Institute, Department of Energy, Consortium for Electric Reliability Technology Solutions, and Power System Engineering Research Center, but improved integration of these efforts is required. . . . Develop dynamic systems technology in conjunction with response demonstrations now being outlined as part of an energy efficiency initiative being formed by EPRI, the Edison Electric Institute, and DOE. These systems would allow interactive control of consumer loads. . . . Develop multilayer control strategies that include capabilities to island and self-heal the power delivery system. This program should involve close cooperation with the electric power industry, building on work in the Wide Area Management System, the Wide Area Control System, and the Eastern Interconnection Phasor Project. . . . Develop improved energy storage that can be deployed as dispersed systems. The committee thinks that improved lithium-ion batteries have the greatest potential. The development of such batteries, which might become commercially viable through use in plug-in hybrid electric vehicles, should be accelerated.</p>	<p>A demonstration has been successfully conducted. Considerable work is still needed on developing and implementing an adequate program of funding and other support for recovery transformers.</p> <p>Limited progress has been made on selected items.</p>

NOTE: NRC (2012) was undertaken for the Department of Homeland Security. Progress has been limited on a number of the recommendations that are listed on page 6 of that report.  
SOURCE: NRC (2012).

is to refine the process, further moving cyber restoration from an ad hoc exercise to an engineering process.

**Recommendation 6.12:** The Department of Energy should develop a high-performance utility network simulator for use in cyber configuration and testing. There is, to date, no flexible, peta-scale utility industrial control system simulator that offers sufficient fidelity for testing intrusion detection, anomaly detection, software defined network controls, and other aspects of utility operations. The closest systems to date take a “hardware-in-the-loop” approach. While this offers some apparent advantages in terms of fidelity, it is too time consuming and expensive to test a wide range of scenarios in such a system. A purely virtual system is necessary.

**DISRUPTIONS THAT INVOLVE ONLY PHYSICAL DAMAGE**

There are few hazards that cause *only* physical damage to the electricity system. Of principal concern is the threat of a well-coordinated and executed physical attack. This was the subject of a 1990 Office of Technology Assessment report (OTA, 1990) and a more recent National Research Council report, *Terrorism and the Electric Power Delivery System* (NRC, 2012). While distribution and transmission equipment have been the target of attacks internationally, the Metcalf incident (described in Chapter 3) is one of the few cases in the United States, although the event was modest in scale and did not disrupt electricity service.

A terrorist attack on the towers and poles of the transmission infrastructure could disrupt service over a large area.

However, utilities are well practiced at rebuilding lines and replacing poles, and it is unlikely that such an outage would be of long duration. The situation is very different for an attack on substations and especially high-voltage transformers. As noted in *Terrorism and the Electric Power Delivery System*, a terrorist attack carried out in a carefully planned way by people who knew what they were doing could “deny large regions of the country access to bulk system power for weeks or even months. An event of this magnitude and duration could lead to turmoil, widespread public fear, and an image of helplessness that would play directly into the hands of the terrorists. If such large extended outages were to occur during times of extreme weather, *they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold*” (NRC, 2012).

Table 6.1 revisits the recommendations made by that report and summarizes the present state of affairs. Unfortunately, the ubiquity of grid assets and their inherent vulnerability make it too costly to achieve a comprehensive high level of security. Resources are prioritized on those assets where improved security will yield the greatest improvement. Efforts to improve security at key assets should proceed alongside efforts to stockpile replacement equipment and develop and deploy temporary recovery assets.

**Finding:** The power system continues to be vulnerable to physical attack by terrorists. Some progress has been made in making the system more resilient in the face of this hazard—for example, through physical security standards such as NERC CIP-014—but much remains to be done. Several



strategies (e.g., high-voltage replacement transformers) that reduce vulnerability to terrorist events also reduce the system's vulnerability to a range of natural hazards.

**Recommendation 6.13:** Efforts by the Department of Energy and the Department of Homeland Security, in conjunction with the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation, and the electric industry, should be redoubled to reduce the vulnerability of the power system to terrorist attacks (paying particular attention to topics in Table 6.1 that have not yet been adequately addressed).

## DISRUPTIONS THAT CAUSE BOTH PHYSICAL AND CYBER DAMAGE

Restoration of electric service from a system that has sustained both physical damage (e.g., a damaged transformer) and compromised monitoring and control systems (e.g., SCADA and EMS disrupted) will require greater reliance on manual inspection and operation, which can slow the pace of damage assessment and recovery. Thus, recovery from a coordinated cyber-physical attack may proceed slowly if operators suffer diminished situational awareness and have to dispatch linemen to assess damage. The principal concern across the industry is the potential for a well-informed state actor or terrorist group to execute a coordinated cyber-physical attack, the so-called structured adversary. Both cyber and physical attacks can be combined, targeted toward system components that cause the most damage or are most difficult to replace, and carried out repeatedly and perhaps with the explicit intent of hindering restoration.

EPRI has developed scenarios of coordinated cyber-physical attacks targeting generation, transmission, and distribution systems that can be used by operators and asset owners to test their readiness and improve planning and drilling (EPRI, 2012). More recently, NERC coordinated more than 100 participating organizations in the biennial distributed-play exercise GridEx III, which practiced response and recovery from a series of hypothetical cyber and physical attacks (NERC, 2016b). Such planning and drilling exercises are a valuable industry practice; however, the level of sophistication of attacks may continue to grow along with the number of vulnerable cyber and physical targets.

**Recommendation 6.14:** Utilities, with support from federal and state government, should continue to expand joint cyber-physical recovery exercises. These should emphasize, among other things, the maintenance of cyber protection during the chaotic period of physical restoration. The need to reconfigure electrical systems during a disaster requires changes to the industrial control system. It is frequently necessary to disable elements of the cybersecurity systems while the state of the grid is in flux. Research should be done on how to maintain a higher level of security during this period. This

may involve operation in default modes or with analog controls to some extent until cybersecurity can be reestablished.

## OPPORTUNITIES TO IMPROVE RESTORATION

### Other Technologies and Operations That Improve Restoration

Though many of the technologies discussed in Chapter 4 are intended to reduce the likelihood and extent of outages, many of these technologies also directly aid in the restoration stage. Improvements from advanced sensing, controls, and analytics have reduced outages and quickened restoration. In particular, distribution system automation and adaptive islanding are examples of where these technologies can play a role in improving restoration. Further, while these technologies help in the resilience of the electric system, these technologies also improve the reliability of the system to small, localized outages.

### Improving Resilience by Learning from Past Events

The final step in restoration is to reflect on and analyze the experience to improve future restoration efforts. Often restoration from a large-area, long-duration outage is viewed as a unique effort. Nonetheless, it is certain that, even in the midst of a great disaster, another similar outage will follow. In 2005, Katrina seemed a nonpareil event, but Superstorm Sandy followed a mere 7 years later. The industry can and must plan for disaster recovery, but only real disasters stress the plans and expose their gaps and weaknesses. Disasters provide a genuinely unique opportunity to learn.

For most large-area, long-duration outages, there is an after-action report that, for the most part, reads like a historical piece rather than a technical study aimed at process improvement. These reports accurately describe what occurred and what was done (when, where, and by whom) as well as contain a number of short narratives related to particular successes or failures. While this information is useful, even essential, the idiosyncratic approaches make it difficult to identify more general process improvements across multiple events. Outside of the electricity industry, other sectors have developed sophisticated investigation procedures and even maintain full-time, well-trained staff whose only job is to investigate major incidents. The National Transportation Safety Board Investigative Process<sup>8</sup> is solely focused on improving safety and since the Board has no regulatory or enforcement powers, its conclusions cannot be used in litigation. The committee believes that the electricity sector can improve its own investigations by learning from the National

<sup>8</sup> The National Transportation Safety Board Investigative Process is described at <https://www.nts.gov/investigations/process/Pages/default.aspx>, accessed July 11, 2017.

*RESTORING GRID FUNCTION AFTER A MAJOR DISRUPTION*

Transportation Safety Board and potentially creating a similar institutional structure.

Part of the problem is the lack of a general restoration model to provide a common framework for learning. A simple, initial framework was proposed earlier in this chapter, and extension and elaboration of that framework could be very useful in structuring the learning process. Two additional problems are as follows: (1) There is no national process or organization to systemize the integration of studies, and (2) there is insufficient rigor to data collection. The following sections describe a general process for collecting information on the failures and shortcomings in disaster restoration.

### **Step 1: Compile High-Level Facts That Describe the Event**

Step 1 is performed by the study team. A summary should be prepared detailing the essential known facts, including a description of the event, high-level summary of known impacts (e.g., where power was lost and for how long), the grid-level drivers of power loss, the organizations involved with restoration and their activities, a timeline of restoration activities, notable successes and failures, and a list of questions raised. From these facts, a series of maps, organization charts, and information flow diagrams should be prepared. This will provide a guide for the research and a common understanding of the event that can be shared among all of the participants in the research.

### **Step 2: Conduct Interviews**

Beginning with the above summary, a series of interviews with a large number of individuals from all organizations involved in the restoration should be undertaken by the study team. The interviews should focus on what the organization did, as well as its inputs and outputs.

### **Step 3: Perform Synthesis**

The synthesis phase is conducted by the study team and supplemented by subject-matter experts as needed. The synthesis phase extends the event summary by using information from the interviews. The results are summarized in a narrative that incorporates a number of graphics. The graphics include an “entity relationship diagram” (ERD); diagrams of material flows, equipment flows, and information flows; and any other charts the study team deems necessary. The ERD is crucial, as it lists all of the entities involved in restoration, from government, utility, and other private sector groups, and documents their interactions through arrows. For example, the governor’s office (entity) may direct (relationship) to the National Guard (entity). The actual flows of material, equipment, and information overlay the ERD. The reduction of the narrative to these artifacts ensures rigor in and understandability of the analysis.

### **Step 4: Conduct Special Engineering Studies**

Special engineering studies are conducted by technical teams assembled for each study. Electrical disasters and remediation are, to a large extent, studies in organization, communication, and coordination. They are at root, however, serious exercises in engineering. Much of the process described here is directed at organizational and process improvement, which is important because it underpins the response to all disasters, but it is just as important to learn about the design and operation of the grid. These elements must be part of the learning process. Based on the recommendations of the interviews, special engineering studies should be initiated. An example that is particularly important is in understanding the transmission grid. Despite its immense scale, it is a precision machine that requires careful harmonization. The studies may look at things like cyber and physical black start, the repair of analog versus digital components in flooded substations, repair of underground laterals in flooded areas, structure failure mode and possibly the need for redesign, and a host of other subjects. Special subjects should be defined in the study phase when they are essential to understanding the restoration or when the restoration presents an opportunity to learn about the grid and how to improve it. Superstorm Sandy provided an unparalleled opportunity to study grid physics at a large scale, and Katrina provided may examples of restoration of flooded substations.

### **Step 5: Review and Distribute Widely**

All parties involved in grid restoration should be involved in review and socialization. This includes individuals and organizations not impacted by the disaster or involved in its restoration. The synthesis report should be widely distributed and reviewed at meetings in a process of improvement and refinement. This will likely span several months.

### **Step 6: Generalize and Integrate**

This step is conducted by a team developed specifically for this purpose but should involve a few members of the study team. The purpose of the final step is to take the specific analysis that comes from Step 5 and use it to improve the general restoration model, asking which lessons have value beyond simply understanding what occurred.

### **Special Studies—Cascading Failures on the Bulk Power System**

The reliability of U.S. electric power systems has been high enough that the rare occurrences of major blackouts have been prominent national and even international news items. Often, the circumstances leading up to a major system failure include multiple individual factors, each of which alone would have little or no significant impact but when



combined conspire to impact the integrity of the system. In the past, such combinations have resulted through coincident occurrence of unrelated events. For example, during the August 14, 2003, blackout, there were four root causes identified (UCPSOTF, 2004). In the future, events could also be brought together through malevolent synergy. The job of an outage investigation team is to sift through all of the evidence to determine the root causes of the larger system failure and extract lessons for future improvement.

The first step in investigating an incident is to accurately reconstruct the sequence of events. Determining the sequence of events can be a time-consuming process. The first step is gathering all of the data to support the investigation team's evidence-building process (Dagle, 2006). Myriad data sources can provide useful information to support this phase of the investigation. Among the most valuable sources of information are operational logs, records of sequence of events, digital fault recorder output, protective relaying event information, synchrophasor data history, and other similar records of real-time information. The accuracy and precision of these event logs can be critical during cascading events, allowing investigators to sift through the initiating actions and subsequent responses. In the past, significant difficulties have arisen in gathering the data to support the investigation team (Dagle, 2004). The good news is that with the advent of modern power system measurement technology, it is becoming much easier to collect data with microsecond-class measurement accuracy, which is often of ample temporal resolution to be able to accurately determine the sequence of events.

Once the sequence of events is organized, it is valuable to separate it into slower events leading up to the cascading failure and faster events that are occurring during the cascading failure itself. Normally the role of human operators is only relevant during the slower events, and automatic controls are involved in the faster sequences associated with the later stages of the cascading failure.

Particularly with the automated controls, it is necessary to understand the relationship among the various steps in the sequence of events. Characterizing the reason behind any automatic control action helps to develop a deeper understanding of the sequence of events and the chain of events that led up to the cascading failure sequence. This often involves a detailed assessment of protection and other control devices to determine why they operated as well as how their operation contributed to subsequent actions in the sequence of events.

Finally, after considering the sequence of events, and earlier actions that contributed to later actions, the process of root cause determination can be made. It is important in this process to understand that actions taken in advance of the event could be a key root cause finding. For example, inadequate vegetation management, rather than a ground fault to a tree, might be a root cause.

Another important consideration is the degree to which infrastructure damage will prevent rapid restoration of

electricity service. As disruptive as widespread blackouts can be, much worse events are possible. Under several different types of circumstances, electric power systems could be damaged well beyond the level of normal design criteria for maintaining reliability (OTA, 1990). The threats of terrorism, severe storms, and other phenomena, such as geomagnetic disturbances, have increasingly become major concerns to the government and the commercial utility industry. The regulations and policies to mandate how the nation would respond to such an event, or even define who is in charge, are still evolving.

**Finding:** Analysis of large-area, long-duration outages requires an enormous amount of high-precision data. Provision for the collection of these data could be in place before an event. Fundamentally, it is the responsibility of each organization involved in operating the system to conduct event investigations, gather lessons learned, and apply those lessons to minimize the likelihood of subsequent similar events. NERC has jurisdiction and responsibility to conduct investigations of outages involving the bulk power system. Particularly for events that involve multiple organizations, NERC brings tremendous value to the process by assembling outside expertise that cuts across organizational boundaries.

**Recommendation 6.15:** The North American Electric Reliability Corporation, the Federal Energy Regulatory Commission, and relevant regional- and state-level organizations should improve the investigation process of large-scale losses of power with the objective of disseminating lessons across geographical and jurisdictional boundaries. Experiences from outside organizations such as the National Transportation Safety Board should inform this work. To further improve the investigation process, the committee recommends that organizations involved in electricity system operation improve restoration through the following:

- Better and more uniform calibration of recording instruments, including precise time synchronization.
- Pre-defined data requirements to support incident investigations using standard data formats.
- Pre-work logistical details (e.g., prior establishment of confidentiality agreements).
- Infrastructure to support centralized blackout investigations.
- Creation of a data warehouse with servers and databases to store and process the incoming data, support the investigation team, and manage data inventory.
- Defined data categories (to readily track and follow-up on data gaps).
- Automated disturbance reporting.
- Routine collection of transmission and generation events.

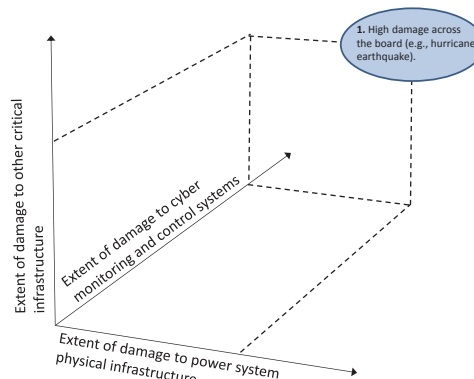
- Improved mechanics of data formats, exchange protocols, and confidentiality issues that can be worked out and tested on an ongoing basis.
- Blackout data that are collected in a matter of hours rather than a matter of days or weeks.

## REFERENCES

- Ball, B. 2006. Rebuilding electrical infrastructure along the Gulf Coast: A case study. *The Bridge: Linking Engineering and Society* 36(1): 21–26.
- CREC (Cuivre River Electric Cooperative). 2016. “Power Restoration Plan.” <https://www.cuivre.com/content/power-restoration-plan>. Accessed July 17, 2017.
- Dagle, J.E. 2004. Data management issues associated with the August 14, 2003 blackout investigation. *IEEE Power Engineering Society General Meeting* 2: 1680–1684.
- Dagle, J.E. 2006. Postmortem analysis of power grid blackouts: The role of measurement systems. *IEEE Power & Energy Magazine* 4(5): 30–35.
- DHS (Department of Homeland Security). 2012. *Recovery Transformer (RecX) Demonstration* [Video file]. <https://www.dhs.gov/science-and-technology/recx-demo-video>. Accessed July 11, 2017.
- DHS. 2014. *Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry*. <https://www.dhs.gov/sites/default/files/publications/RecX%20-%20Emergency%20Spare%20Transformer%20Strategy-508.pdf>.
- DHS. 2016. *National Response Framework*. 3rd Edition. <https://www.fema.gov/national-response-framework>. Accessed July 13, 2017.
- DOE (Department of Energy). 2015. “Modernizing the Electric Grid.” *Quadrennial Energy Review First Installment: Transforming U.S. Energy Infrastructures in a Time of Rapid Change*. <http://energy.gov/epsa/downloads/quadrennial-energy-review-first-installment>. Accessed July 13, 2017.
- DOE. 2016. *Promoting Innovation for the Design of More Flexible Large Power Transformers*. <https://energy.gov/oe/articles/promoting-innovation-design-more-flexible-large-power-transformers>. Accessed July 11, 2017.
- DOE. 2017. *Quadrennial Energy Review: Transforming the Nation's Electricity System: The Second Installment of the QER*. <https://energy.gov/epsa/downloads/quadrennial-energy-review-second-installment>. Accessed July 13, 2017.
- EEI (Edison Electric Institute). 2016. *Understanding the Electric Power Industry's Response and Restoration Process*. [http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/documents/ma\\_101final.pdf](http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/documents/ma_101final.pdf).
- EPRI (Electric Power Research Institute). 2010. “Development of Power System Restoration Tool Based on Generic Restoration Milestones.” <https://www.epri.com/#/pages/product/000000000001020055/>. Accessed July 13, 2017.
- EPRI. 2012. “Coordinated Cyber-physical Attacks, High-Impact Low-Frequency (HILF) Events, and Risk Management in the Electric Sector.” <http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001025861>. Accessed July 13, 2017.
- EPRI. 2013. “Enhancing Distribution Resiliency: Opportunities for Applying Innovative Technologies.” <https://www.epri.com/#/pages/product/000000000001026889/>. Accessed March 17, 2017.
- ESCC (Electricity Subsector Coordinating Council). 2016. “Overview.” <http://www.electricitysubsector.org/>. Accessed December 15, 2016.
- Fugate, W.C. 2012. “Hurricane Sandy: Response and Recovery Progress and Challenges.” Hearing Before a Subcommittee of the Committee on Appropriations, United States Senate, 112th Congress, December 5.
- Lacey, S. 2014. “Resiliency: How Superstorm Sandy Changed America's Grid.” *GreentechMedia*, June 10. <https://www.greentechmedia.com/articles/featured/resiliency-how-superstorm-sandy-changed-americas-grid>. Accessed July 13, 2017.
- Mandiant. 2016. “M-Trends.” <https://www2.fireeye.com/PPC-m-trends-2016-trends-statistics-mandiant.html>. Accessed July 11, 2017.
- Miller, C., M. Martin, D. Pinney, and G. Walker. 2014. *Achieving a Resilient and Agile Grid*. [http://www.electric.coop/wp-content/uploads/2016/07/Achieving\\_a\\_Resilient\\_and\\_Agile\\_Grid.pdf](http://www.electric.coop/wp-content/uploads/2016/07/Achieving_a_Resilient_and_Agile_Grid.pdf).
- NASEM (National Academies of Sciences, Engineering, and Medicine). 2016. *Electricity Use in Rural and Islanded Communities: Proceedings of a Workshop*. Washington, D.C.: The National Academies Press.
- NERC (North American Electric Reliability Corporation). 2016a. *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*. <https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf>.
- NERC. 2016b. *Grid Security Exercise*. <http://www.nerc.com/pa/CI/CIP Outreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.
- NRC (National Research Council). 2012. *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press.
- NYSEG (New York State Electric and Gas Corporation) and RGEC (Rochester Gas and Electric Corporation). 2016. *Electricity Utility Emergency Plan*. <https://www.nyseg.com/MediaLibrary/2/5/Content%20Management/Shared/SuppliersPartners/PDFs%20and%20Docs/NYSEG%20and%20ERGE%20Electric%20Utility%20Emergency%20Plan.pdf>.
- Olearczyk, M. 2013. *Airborne Damage Assessment Module (ADAM)*. Electric Power Research Institute 2013 Distribution System Research Portfolio. [http://mydocs.epri.com/docs/Portfolio/PDF/2013\\_P180.pdf](http://mydocs.epri.com/docs/Portfolio/PDF/2013_P180.pdf).
- OTA (Office of Technology Assessment). 1990. *Physical Vulnerability of Electric System to Natural Disasters and Sabotage, OTA-E-453*. Washington, D.C.: U.S. Government Printing Office.
- Parfomak, P.W. 2014. *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*. <https://fas.org/sgp/crs/homesecc/R43604.pdf>.
- PJM. 2016. “PJM Manual 36: System Restoration.” <http://www.pjm.com/~media/documents/manuals/m36.ashx>. Accessed July 13, 2017.
- UCPSOTF (U.S.–Canada Power System Outage Task Force). 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendation*. <https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>.

## ANNEX TABLES

**TABLE 6A.1** Variation in Restoration Activities Across the Six Stages of the Life Cycle of an Outage Characterized by Damage to Physical Components, Monitoring and Control Systems, and Supporting Infrastructure, As Indicated in the Upper Right Corner of Figure 3.2



	Hurricanes and Tropical Storms	Floods
	<p>Area impacted: Typically very large</p> <p>Damage to aboveground assets: Poles, towers, substations</p> <p>Damage to customer assets: Extensive</p> <p>Limits to access and mobility: Major blockage</p> <p>Event warning: Days</p> <p>Risk assessment: Can be identified beforehand</p> <p>Rate of propagation: Slow</p>	<p>Area impacted: Typically very large</p> <p>Damage to aboveground assets: Poles, towers, substations</p> <p>Damage to customer assets: Extensive</p> <p>Limits to access and mobility: Major blockage</p> <p>Event warning: Days</p> <p>Risk assessment: Can be identified beforehand</p> <p>Rate of propagation: Slow</p>
<b>Plan</b>	<p>Individual utilities plan for hurricanes and tropical storms based on their experience and historical hurricane tracks, although these tracks may be trending more northerly in the Atlantic, placing the Mid-Atlantic states and New England at greater risk than in the past. Utilities are experts in identifying their specific vulnerable assets. During this phase, utilities should establish and refresh mutual aid agreements, create owned and shared inventory, train crews, conduct exercises, and communicate with customers regarding emergency preparedness.</p>	<p>More than any other disaster, floods are subject to statistical analysis, and utilities plan based on FEMA flood maps. Some adjustment should be made if there has been substantial reduction in forest cover or if there has been substantial development in the impacted watershed. Consideration should also be given to how, in light of climate change, future flood risk may be different from historical risk. To the extent possible, critical assets should not be located in identified flood plains, but there are numerous legacy assets exposed to flood risk. Floods in major river basins tend to be slow rising and slow receding, with lesser hydrostatic force. In contrast, canyon flooding (largely in western mountains) tends to be fast rising with short notice, forceful, and quick to recede. In either case, assets at risk can be identified and measures taken to reduce risk such as elevating them above the flood or building coffer dams. Plans should be made to replace assets in flood plains.</p>
<b>Prepare</b>	<p>Hurricane wind and rain forecasts with high uncertainty are available up to 1 week in advance, which is sufficient time to elevate or downgrade risk. When risk is elevated, staffing for the emergency can be refined, and mutual aid agreements can be activated. Flood forecasts are available only 3 to 4 days in advance, and peak flooding frequently follows the event.</p>	<p>River basin flood forecasts are available 3 to 4 days in advance. Many flash floods occur with effectively no warning; however, if major rain events are forecast for canyon areas, utilities may place crews on standby. When a flood is forecast in a river basin, it is possible to forecast which areas and assets are most likely to be affected. General restoration plans can be made more specific, and mutual aid agreements and emergency operations centers can be activated. Lists of materials, supplies, and equipment can be developed, procured, and staged.</p>
<b>Event</b>	<p>Relatively little can be done on distribution systems during the comparatively short duration of the event. Transmission systems must be adjusted as loads, generators, and transmission lines drop off the grid. Utilities develop an understanding of the extent of damage and customer outages and develop specific plans for remediation, building on the general planning. Government support organizations monitor conditions and establish and exercise lines of communications with utilities and with each other. Limited actions should be taken by utilities only when safety is an issue.</p>	<p>Major river floods are long-duration events that move down a river basin. Restoration can start upstream while the event is still evolving downstream, and some protective measures can be undertaken as water rises. Before restoration begins in an area, the plans can be improved and refined with emphasis on the temporal sequencing. Communications and coordination should be established and exercised.</p>

	Hurricanes and Tropical Storms	Floods
<b>Endure</b>	The endurance phase is the period from when the storm passes to the start of restoration. Unless there is flooding, restoration can begin immediately. If there is a delay, the time should be spent moving crews into position to the extent that the condition of the roads and safety considerations allow. Effort should also be made to improve the assessment of the state of conditions, to refine plans, and to refine requests for support from and coordination with other organizations, including other utilities and government organizations. This involves the high level such as governors' offices, but also the crews on the ground, as per informing police and fire departments about the utility staff who will be working in their area. If specialized equipment is needed, arrangements should be made for acquisition and staging for deployment.	The endurance phase for a flood at one point can be very short in areas where the grade of a river is steeper or long in low-lying flat areas. Work begins in an area as soon as the water recedes, allowing restoration.
<b>Restore</b>	Restoration is the most visible phase of the event. Crews are on the streets working. While this is a difficult and costly phase, it is one that most utilities are familiar with and good at. If there are many trees and other obstacles in the street, they must be cleared to gain access to facilities. Utilities and the linemen know how to clear access, set poles, erect towers, string conductors, and clean and repair substations. The goal of management and support organizations (including governmental) is to ensure that the line crews are used effectively. They must be dispatched to the areas where their work will have the greatest impact, considering what is doable, and placed in a sequence of restoration activities. Management should work the supply chain to be sure that crews have the equipment, parts, and supplies (including fuel) they need to execute the necessary repairs. Crews must be provided with provisions, including food and housing, and amenities, such as electrical and phone service and access to health services for the injuries that are inevitable in this dangerous physical work. Experience has shown that taking care of the families left behind when crews are deployed is an important factor in enabling them to work effectively.	Flood restoration can take a very long time. In the absence of wind, poles and towers are not typically damaged; nonetheless, the ground can be softened and some distribution and transmission failures may occur. Manholes are flooded and must be pumped out. Underground lines and associated gear sometimes survive intact but often are damaged to the point of needing costly and time-consuming replacement. Flooded substations are difficult to restore. Analog equipment can sometimes be cleaned, dried, and returned to service, but digital devices typically need replacement. Underground vaults are problematic as they are difficult to drain and dry, can accumulate deep mud, and are more difficult to move equipment in and out of. All of this, however, is work utilities know and are well equipped to manage. The key, as noted in the discussion of hurricanes, is to provide broad support to the crews.
<b>Recover</b>	Hurricanes damage communities, not just utilities. Utilities must be part of the community restoration, perhaps lasting years. Rebuilding is an opportunity for improving.	Floods damage communities, not just utilities. Utilities must cooperate with other entities in the restoration as, for example, in repairing or replacing civil and safety infrastructure.
	Earthquakes	Winter Storms
	Area impacted: Limited to extensive Damage to aboveground assets: Poles, towers, substations Damage to customer assets: Limited to extensive Limits to access and mobility: Major blockage Event warning: Seconds to minutes Risk assessment: Difficult Rate of propagation: Fast	Area impacted: Regional Damage to aboveground assets: Lines, poles, towers Damage to customer assets: Limited Limits to access and mobility: Potential blockage Event warning: Days Risk assessment: Straightforward Rate of propagation: Slow
<b>Plan</b>	Earthquake risk is well mapped, and utilities routinely consider earthquake risk in siting and planning processes. Methods for earthquake-survivable construction are well researched. Major plants (e.g., North Anna Nuclear Power Station) have survived earthquakes with no damage, though safety considerations have taken them off-line for an extended period. Planning consists of maintaining adequate parts inventories.	Utilities operating in regions subject to winter storms often design systems components, such as transmission towers and lines, to be able to withstand greater amounts of precipitation and wind compared to other areas.
<b>Prepare</b>	There is work on developing a near-term warning capability for earthquakes, but presently most occur with no useful warning.	Winter storm forecasts provide several days' warning that allows for arrangement of mutual aid.
<b>Event</b>	Earthquakes are of short duration. No action during the earthquake is practical.	Some final preparation is possible during the event as outages are mapped. Transmission system operators must rebalance to accommodate failing loads and distribution systems.
<b>Endure</b>	Restoration can begin immediately.	Delay in the start of restoration is possible if the roads are blocked or ice-covered.

*continued*

TABLE 6A.1 Continued

	Earthquakes	Winter Storms
<b>Restore</b>	Restoration consists of familiar utility construction but can be severely hampered by damage to supporting infrastructure. Roads and bridges can be blocked or torn away, natural gas pipelines can break, and fuel storage can rupture. Electricity system restoration is executed as part of a broader restoration effort, and coordination among federal, state, and local government, as well as utility decision makers, is essential. Shortages of materials and equipment may result in competition for scarce resources, and availability will vary geographically. Even access to food and water may be a challenge in some remote areas. There is substantial risk that the homes and families of crews may be impacted or imperiled, undermining their ability to commit to utility restoration activities. Mutual aid from unaffected areas is essential.	Restoration following winter storms is standard utility work. Mutual aid is beneficial, and due to the generally smaller geographic extent of such storms, there are fewer issues in supporting the crews or marshalling supplies than are faced during restoration from hurricanes and earthquakes. Cold temperatures do reduce effectiveness of line crews.
<b>Recover</b>	Utility restoration can be completed well in advance of the general commercial and civil infrastructure. Utility capabilities are enablers of recovery.	Winter storms do not typically inflict lasting damage on infrastructure and enablers of economic recovery.
	Tornadoes	Geomagnetic Disturbances
	Area impacted: Limited to clustered Damage to aboveground assets: Poles, towers, substations Damage to customer assets: Serious but contained Limits to access and mobility: Minor blockage Event warning: Seconds to minutes Risk assessment: Regionally known Rate of propagation: Fast	Area impacted: Very large Damage to aboveground assets: Transformers, substations Damage to customer assets: Limited Limits to access and mobility: None Event warning: Minutes to days Risk assessment: Costly Rate of propagation: Very fast
<b>Plan</b>	Utilities in high-risk areas are aware of the peril and have likely dealt with tornadoes in the past. The focus in planning is on inventory of aboveground assets and mutual assistance. Unlike some other causes, transmission and generation assets are at risk of damage from tornadoes.	Risk assessment is nascent and based on highly uncertain estimates of frequency and intensity, but methods to harden the grid are available. Replacement transformers and other vulnerable components can be stockpiled but may be too expensive to be forward deployed.
<b>Prepare</b>	The incidence of weather conditions likely to spawn tornadoes can be provided 1 day to several hours in advance. There is little time to prepare, except to bring crews to a state of readiness and fully man response centers.	Solar weather warning systems can provide some notice, allowing for minimal preparation, but there is generally insufficient time to move crews.
<b>Event</b>	Events are of such short duration that there is no practical action during the event, except that transmission operators may have to adjust to limit impact.	The building up of current on long lines can trigger operational changes to protection systems, particularly shedding load to desaturate transformers.
<b>Endure</b>	Restoration can generally begin immediately after the event passes.	Restoration can begin immediately.
<b>Restore</b>	Customer property may be destroyed alongside utility assets, which means that there may be no immediate need to restore power to the affected area. Nonetheless, the tornado may damage a transmission corridor or section of the distribution grid essential to providing service to unaffected areas. The work is familiar to utilities and, in the case of tornadoes, the impact is sufficiently localized that there is less difficulty in provisioning and supporting crews. There are likely to be intact facilities within a few miles or tens of miles of the worksite.	There is no precedent for a large-scale geomagnetic disturbance event. If the impact is very large, there may be shortages of major components, particularly large transformers due to the long lead time in building and acquiring these.
<b>Recover</b>	Tornadoes do very serious damage to the impacted community so that the recovery period can be extensive after the immediate restoration is completed. Utilities must participate in planning this recovery.	Recovery is not a factor. Extensive damage beyond the grid is unlikely since long lines are needed to build damaging current level.



**TABLE 6A.2** Restoration Activities Across the Six Stages of the Life Cycle of an Outage from a Cyber Attack

Area Impacted	Feeder Level to System Level
Damage to aboveground assets	Cyber assets will certainly be compromised, perhaps beyond restoration. Control actions initiated by the pernicious actor may create a wide range of physical damage up to and including generators. In addition, “smart” components may be compromised in a way that they are no longer controllable. Such damage may be irreversible or compromise trust in the device so that it may not be used safely. This damage to the electronic aspects of a device is functionally equivalent to physical damage.
Damage to customer assets	Limited except, possibly, to smart meters. Meters are owned by the utility but are associated with a specific customer. If the meter includes a local wireless connection for home automation, there are potential attack strategies which may do damage to customer systems, but no such Internet of Things attack has been successful.
Limits to access and mobility	None.
Event warning	Potentially months.
Risk assessment	Cyber N-1 and N-2 analyses should become standard practice.
Rate of propagation	Slow from breach to first action, very fast from first action.
<b>Plan</b>	Planning for cyber attack is a routine part of utility operations. It tends to focus, however, on prevention rather than restoration. The emphasis in restoration is on reestablishing the operational capability of sensor, computational, and communications assets; reestablishing state; and gaining confidence in the integrity of the systems and the information they manage. Planning for cyber restoration should be planned and practiced.
<b>Prepare</b>	Systems must be improved to react more effectively to new threat information. Updated threat information is provided daily, but the systems to move this information into quick action at a utility cannot make immediate use of the information. Much of it must work its way through cybersecurity software and service providers.
<b>Event</b>	A cyber event may last several months. During the period from breach to action, the utility may be able to sever access by malicious actors, preventing damage.
<b>Endure</b>	Restoration can begin immediately on detection.
<b>Restore</b>	Methods for manual operation and restoration systems should be developed in advance. Fast reaction cyber teams should be on call.
<b>Recover</b>	Not applicable.

## 7

## Conclusions

No single entity is responsible for, or has the authority to implement, a comprehensive approach to assure the resilience of the nation's electricity system. Chapter 2 described the complex structure, asset ownership, and regulatory system of the current electricity system and how the changing nature of the electricity system provides both opportunities and challenges for system resilience. Because most parties are preoccupied dealing with short-term issues, they neither have the time to think systematically about what could happen in the event of a large-area, long-duration blackout, nor do they adequately consider the consequences of large-area, long-duration blackouts in their operational and other planning or in setting research and development priorities. Hence the United States needs a process to help all parties better envision the consequences of low-probability but high-impact events precipitated by the causes outlined in Chapter 3 and the system-wide effects discussed in Chapter 5. The specific recommendations addressed to particular parties that are provided in the report (especially in Chapters 4 through 6) will incrementally advance the cause of resilience. However, these alone will be insufficient unless the nation is able to adopt a more integrated perspective at the same time. Thus, this chapter provides a series of overarching recommendations that build upon the detailed recommendations contained within this report.

### OVERARCHING INSIGHTS AND RECOMMENDATIONS

The first strategy that should be pursued to enhance the resilience of the system is to make sure that things already in place will work when they are needed. One of the best ways to do that is to conduct drills with other critical infrastructure operators through large-scale, multisector exercises. Such exercises can help illuminate areas where improvements in processes and technologies can substantively enhance the resilience of the nation's critical infrastructure.

**Overarching Recommendation 1:** Operators of the electricity system, including regional transmission organizations,

investor-owned utilities, cooperatives, and municipally owned utilities, should work individually and collectively, in cooperation with the Electricity Subsector Coordinating Council, regional and state authorities, the Federal Energy Regulatory Commission, and the North American Electric Reliability Corporation, to conduct more regional emergency preparedness exercises that simulate accidental failures, physical and cyber attacks, and other impairments that result in large-scale loss of power and/or other critical infrastructure sectors—especially communication, water, and natural gas. Counterparts from other critical infrastructure sections should be involved, as well as state, local, and regional emergency management offices.

The challenges that remain to achieving grid resilience are so great that they cannot be achieved by research- or operations-related activities alone. While new technologies and strategies can improve the resilience of the power system, many existing technologies that show promise have yet to be fully adopted or implemented. In addition, more coordination between research and implementation activities is needed, building on the specific recommendations made throughout this report. Immediate action is needed both to implement available technological and operational changes and to continue to support the development of new technologies and strategies.

**Overarching Recommendation 2:** Operators of the electricity system, including regional transmission organizations, investor-owned utilities, cooperatives, and municipals, should work individually and collectively to more rapidly implement resilience-enhancing technical capabilities and operational strategies that are available today and to speed the adoption of new capabilities and strategies as they become available.

The Department of Energy (DOE) is the federal entity with a mission to focus on the *longer-term* issues of developing and promulgating technologies and strategies to increase

## CONCLUSIONS

the resilience and modernization of the electric grid.<sup>1</sup> At present, two offices within DOE have responsibility for issues directly and indirectly related to grid modernization and resilience.

**Overarching Recommendation 3:** However the Department of Energy chooses to organize its programs going forward, Congress and the Department of Energy leadership should sustain and expand the substantive areas of research, development, and demonstration that are now being undertaken by the Department of Energy's Office of Electricity Delivery and Energy Reliability and Office of Energy Efficiency and Renewable Energy, with respect to grid modernization and systems integration, with the explicit intention of improving the resilience of the U.S. power grid. Field demonstrations of physical and cyber improvements that could subsequently lead to widespread deployment are critically important. The Department of Energy should collaborate with parties in the private sector and in states and localities to jointly plan for and support such demonstrations. Department of Energy efforts should include engagement with key stakeholders in emergency response to build and disseminate best practices across the industry.

The U.S. grid remains vulnerable to natural disasters, physical and cyber attacks, and other accidental failures.

**Overarching Recommendation 4:** Through public and private means, the United States should substantially increase the resources committed to the physical components needed to ensure that critical electric infrastructure is robust and that society is able to cope when the grid fails. Some of this investment should focus on making the existing infrastructure more resilient and easier to repair, including the following:

- The Department of Energy should launch a program to manufacture and deploy flexible and transportable three-phase recovery transformer sets that can be pre-positioned around the country.<sup>2</sup> These recovery transformers should be easy to install and use temporarily

<sup>1</sup> The Department of Homeland Security, the Federal Energy Regulatory Commission, and other organizations also provide critical support and have primacy in certain areas.

<sup>2</sup> As noted in Chapter 6 and in the next section of this chapter, the DOE Office of Electricity Delivery and Energy Reliability is supporting the development of a new generation of high-voltage transformers that will use power electronics to adjust their electrical properties and hence can be deployed in a wider range of settings. The committee's recommendation to manufacture recovery transformers is not intended to replace that longer-term effort. However, the new DOE advanced transformer designs will not be available for some time, and in the meantime the system remains physically vulnerable. While in Chapter 6 the committee notes several government and industry-led transformer-sharing and recovery programs, the committee recognizes that high-voltage transformers represent one of the grid's most vulnerable components deserving of further efforts.

until conventional transformer replacements are available. This effort should produce sufficient numbers (on the order of tens compared to the three produced by the Department of Homeland Security's RecX program) to provide some practical protection in the case of an event that results in the loss of a number of high-voltage transformers. This effort should complement instead of replace ongoing initiatives related to spare transformers.

- State and federal regulatory commissions and regional transmission organizations should then evaluate whether grids under their supervision need additional pre-positioned replacements for critical assets that can help accelerate orderly restoration of grid service after failure.
- Public and private parties should expand efforts to improve their ability to maintain and restore critical services—such as power for hospitals, first responders, water supply and sewage systems, and communication systems.<sup>3</sup>
- The Department of Energy, the Department of Homeland Security, the Electricity Subsector Coordinating Council, and other federal organizations, such as the U.S. Army Corps of Engineers, should oversee the development of more reliable inventories of backup power needs and capabilities (e.g., the U.S. Army Corps of Engineers' mobile generator fleet), including fuel supplies. They should also "stress test" existing supply contracts for equipment and fuel supply that are widely used in place of actual physical assets in order to be certain these arrangements will function in times of major extended outages. Although the federal government cannot provide backup power equipment to everyone affected by a large-scale outage, these resources could make significant contributions at select critical loads.

In addition to providing redundancy of critical assets, transmission and distribution system resilience demands the ability to provide rapid response to events that impair the ability of the power system to perform its function. These events include deliberate attacks on and accidental failures of the infrastructure itself, as well as other causes of grid failure, which are discussed in Chapter 3.

**Overarching Recommendation 5:** The Department of Energy, together with the Department of Homeland Security, academic research teams, the national laboratories, and companies in the private sector, should carry out a program of research, development, and demonstration activities to

<sup>3</sup> In addition to treatment, sewage systems often need to pump uphill. A loss of power can quickly lead to sewage backups. Notably, a high percentage of the hospital backup generators in New York City failed during Superstorm Sandy.

improve the security and resilience of cyber monitoring and controls systems, including the following:

- Continuous collection of diverse (cyber and physical) sensor data;
- Fusion of sensor data with other intelligence information to diagnose the cause of the impairment (cyber or physical);
- Visualization techniques needed to allow operators and engineers to maintain situational awareness;
- Analytics (including machine learning, data mining, game theory, and other artificial intelligence-based techniques) to generate real-time recommendations for actions that should be taken in response to the diagnosed attacks, failures, or other impairments;
- Restoration of control system and power delivery functionality and cyber and physical operational data in response to the impairment; and
- Creation of post-event tools for detection, analysis, and restoration to complement event prevention tools.

Because no single entity is in charge of planning the evolution of the grid, there is a risk that society may not adequately anticipate and address many elements of grid reliability and resilience and that the risks of this system-wide failure in preparedness will grow as the structure of the power industry becomes more atomized and complex. There are many opportunities for federal leadership in anticipating potential system vulnerabilities at a national level, but national solutions are then refined in light of local and regional circumstances. Doing this requires a multi-step process, the first of which is to anticipate the myriad ways in which the system might be disrupted and the many social, economic, and other consequences of such disruptions. The second is to envision the range of technological and organizational innovations that are affecting the industry (e.g., distributed generation and storage) and how such developments may affect the system's reliability and resilience. The third is to figure out what upgrades should be made and how to cover their costs. For simplicity, the committee will refer to this as a "visioning process." While the Department of Homeland Security (DHS) has overarching responsibility for infrastructure protection, DOE, as the sector-specific agency for energy infrastructure, has a legal mandate and the deep technical expertise to work on such issues.

**Overarching Recommendation 6:** The Department of Energy and the Department of Homeland Security should jointly establish and support a "visioning" process with the objective of systematically imagining and assessing plausible large-area, long-duration grid disruptions that could have major economic, social, and other adverse consequences, focusing on those that could have impacts related to U.S. dependence on vital public infrastructures and services provided by the grid.

Because it is inherently difficult to imagine systematically things that have not happened (Fischhoff et al., 1978; Kahneman, 2011), exercises in envisioning benefit from having multiple groups perform such work independently. For example, such a visioning process might be accomplished through the creation of two small national power system resilience assessment groups (possibly at DOE national laboratories and/or other federally funded research and development centers or research universities). However such visioning is accomplished, engagement from staff representing relevant state and federal agencies is essential in helping to frame and inform the work. These efforts should build on the detailed recommendations in this report to identify technical and organizational strategies that increase electricity system resilience in numerous threat scenarios—that is, by preventing and mitigating the extent of large-scale grid failures, sustaining critical services in the instance of failure, and recovering rapidly from major outages—and to assess the costs and financing mechanisms to implement the proposed strategies. Attention is needed not just to the average economy-wide costs and benefits, but also to the distribution of these across different levels of income and vulnerability. It is important that these teams work to identify common elements in terms of hazards and solutions so as to move past a hazard-by-hazard approach to a more systems-oriented strategy. Producing useful insights from this process will require mechanisms to help these groups identify areas of overlap while also characterizing the areas of disagreement. A consensus view could be much less helpful than a mapping of uncertainties that can help other actors—for example, state regulatory commissions and first responders—understand the areas of deeper unknowns.

National labs, other federally funded research and development centers, and research universities do not operate or regulate the power system. At the national level, the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) both have relevant responsibilities and authorities.

**Overarching Recommendation 7A:** The Federal Energy Regulatory Commission and the North American Electric Reliability Corporation should establish small system resilience groups, informed by the work of the Department of Energy/Department of Homeland Security "visioning" process, to assess and, as needed, to mandate strategies designed to increase the resilience of the U.S. bulk electricity system. By focusing on the crosscutting impacts of hazards on interdependent critical infrastructures, one objective of these groups would be to complement and enhance existing efforts across relevant organizations.

As the discussions throughout this report make clear, many different organizations are involved in planning, operating, and regulating the grid at the local and regional levels. By design and of necessity in our constitutional democracy,

## CONCLUSIONS

making decisions about resilience is an inherently political process. Ultimately the choice of how much resilience our society should and will buy must be a collective social judgment. It is unrealistic to expect firms to make investments voluntarily whose benefits may not accrue to shareholders within the relevant commercial lifetime for evaluating projects. Moreover, much of the benefit from avoiding such events, should they occur, will not accrue to the individual firms that invest in these capabilities. Rather, the benefits are diffused more broadly across multiple industries and society as a whole, and many of the decisions must occur on a state-by-state basis.

**Overarching Recommendation 7B:** The National Association of Regulatory Utility Commissioners should work with the National Association of State Energy Officials to create a committee to provide guidance to state regulators on how best to respond to identified local and regional power system-related vulnerabilities. The work of this committee should be informed by the national “visioning” process, as well as by the work of other research organizations. The mission of this committee should be to develop guidance for, and provide technical and institutional support to, state commissions to help them to more systematically address broad issues of power system resilience, including decisions as to what upgrades are desirable and how to pay for them. Guidance developed through this process should be shared with appropriate representatives from the American Public Power Association and the National Rural Electric Cooperative Association.

**Overarching Recommendation 7C:** Each state public utility commission and state energy office, working with the National Association of Regulatory Utility Commissioners, the National Association of State Energy Officials, and state and regional grid operators and emergency preparedness organizations, should establish a standing capability to identify vulnerabilities, identify strategies to reduce local vulnerabilities, develop strategies to cover costs of needed upgrades, and help the public to become better prepared for extended outages. In addition, they should encourage local and regional governments to conduct assessments of their potential vulnerabilities in the event of large-area, long-duration blackouts and to develop strategies to improve their preparedness.

Throughout this report, the committee has laid out a wide range of actions that different parties might undertake to improve the resilience of the United States power system. If the approaches the committee has outlined can be implemented, they will represent a most valuable contribution. At the same time, the committee is aware that the benefits of such a contribution—avoiding large-scale harms that are rarely observed—are easily eclipsed by the

more tangible daily challenges, pressures on budgets, public attention, and other scarce resources. Too often in the past, the United States has made progress on issues of resilience by “muddling through” (Lindblom, 1959). Even if the broad systematic approach outlined in this report cannot be fully implemented immediately, it is important that relevant organizations develop analogous strategies so that when a policy window opens in the aftermath of a major disruption, well-conceived solutions are readily available for implementation (Kingdon, 1984).

## SUMMARY OF DETAILED RECOMMENDATIONS

Underlying the Overarching Recommendations are the numerous, more targeted recommendations presented throughout this report. Here, the committee summarizes and sorts these recommendations by the institutions to which they are directed.

## Recommendations Directed to the Department of Energy

DOE plays a critical role in enhancing the resilience of the grid through research, development, and demonstration programs as well as convening and engagement activities. Much progress has been made, and DOE should sustain and expand many of these efforts.

**Recommendation 1 to DOE:** Improve understanding of customer and societal value associated with increased resilience and review and operationalize metrics for resilience by doing the following:

- Developing comprehensive studies to assess the value to customers of improved reliability and resilience (e.g., periodic rotating service) during large-area, long-duration blackouts as a function of key circumstances (e.g., duration, climatic conditions, societal function) and for different customer classes (e.g., residential, commercial, industrial). (Recommendation 2.1)
- Conducting a coordinated assessment of the numerous resilience metrics being proposed for transmission and distribution systems and seeking to operationalize these metrics within the utility setting. In doing the review, engagement with key stakeholders is essential. (Recommendation 2.2)

**Recommendation 2 to DOE:** Support research, development, and demonstration activities, as well as convening activities, to improve the resilience of power system operations and recovery by reducing barriers to adoption of innovative technologies and operational strategies. These include the following:

- Coordinating with federal and state utility regulators to support a modest grant program that encourages utility



investment in innovative solutions that demonstrate resilience enhancement. These projects should be selected to reduce barrier(s) to entry by improving regulator and utility confidence. (Recommendation 4.1)

- Initiating and supporting ongoing research programs focused on the operation of degraded or damaged electricity systems, including supporting infrastructure and cyber monitoring and control systems, where key subsystems are designed and operated to sustain critical functionality. (Recommendation 4.6)
- Convening transmission and distribution system owners and operators to engage the Federal Aviation Administration proactively to ensure that the rules regulating operation of unmanned aerial vehicles support the rapid, safe, and effective applications of unmanned aerial vehicle technology in electricity restoration activities, including pre-disaster tests and drills. (Recommendation 6.5)
- Continuing to support research and development of advanced large power transformers, concentrating on moving beyond design studies to conduct several demonstration projects. (Recommendation 6.7)

**Recommendation 3 to DOE:** Advance the safe and effective development of distributed energy resources (DERs) and microgrids by doing the following:

- Initiating research, development, and demonstration activities to explore the extent to which DERs could be used to help prevent large-area outages. (Recommendation 4.2)
- Supporting demonstration and a training facility (or facilities) for future microgrids that will allow utility engineers and non-utility microgrid operators to gain hands-on experience with islanding, operating, and restoring feeders (including microgrids). (Recommendation 5.6)
- Engaging the manufacturers of plug-in hybrid electric and fuel cell vehicles to study how such vehicles might be used as distributed sources of emergency power. (Recommendation 5.12)
- Evaluating the technical and contractual requirements for using DERs as part of restoration activities, even when these assets are not owned by the utility, to improve restoration and overall resilience. (Recommendation 6.3)

**Recommendation 4 to DOE:** Work to improve the ability to use computers, software, and simulation to research, plan, and operate the power system to increase resilience by doing the following:

- Collaborating with other research organizations, including the National Science Foundation, to expand support for interdisciplinary research to simulate

events and model grid impacts and mitigation strategies. (Recommendation 4.3)

- Supporting and expanding research and development activities to create synthetic power grid physical and cyber infrastructure models. (Recommendation 4.4)
- Collaborating with other research organizations, including the National Science Foundation, to fund research on enhanced power system wide-area monitoring and control and the application of artificial intelligence to the power system. Such work should include how the human-computer interface and visualization could improve reliability and resilience. (Recommendation 4.8)
- Leading efforts to develop standardized data definitions, communication protocols, and industrial control system designs for the sharing of both physical and cyber system health information. (Recommendation 4.9)
- Developing a high-performance utility network simulator for use in cyber configuration and testing. (Recommendation 6.12)

**Recommendation 5 to DOE:** Work to improve the cybersecurity and cyber resilience of the grid by doing the following:

- Embarking on a research, development, and demonstration program that results in a prototypical cyber-physical-social control system architecture for resilient electric power systems. (Recommendation 4.10)
- Developing the ability to apply physics-based modeling to anomaly detection, which provides real-time or better physics models that derive optimal power flow and monitor performance for more accurate state estimation. (Recommendation 6.8)

### **Recommendations Directed to the Electric Power Sector and the Department of Energy**

There are thousands of operating utilities and electricity system asset owners across the United States, with diverse characteristics and institutional structures, including private investor-owned utilities, cooperatives, and publicly owned entities. These organizations, and the people they employ, are the foundation of a reliable and resilient grid, and many promising demonstrations and initiatives are ongoing across the sector. The industry and DOE have benefitted from a strong relationship, and the committee encourages further collaboration on projects to increase the resilience of the grid.

**Recommendation 6 to the electric power sector and DOE:** The owners and operators of electricity infrastructure should work closely with DOE as follows:

- Develop use cases and perform research on strategies for intelligent load shedding based on advanced

## CONCLUSIONS

metering infrastructure and customer technologies like smart circuit breakers. (Recommendation 4.5)

- Explore the feasibility of establishing contractual and billing agreements with private owners of DERs and developing the ability to operate intact islanded feeders as islanded microgrids powered by utility- and customer-owned generating resources to supply limited power to critical loads during large grid outages of long duration. (Recommendation 5.10)
- Work together to analyze past large-area, long-duration outages to identify common elements and processes for system restoration and define best practices that can be shared broadly throughout the electricity industry. (Recommendation 6.2)
- Identify those components and corresponding events for which pre-event de-energizing of selected assets is the lowest risk strategy and develop regulatory, communication (especially with customers), and other plans that allow such protective action to be implemented. (Recommendation 6.4)
- Expand joint cyber-physical recovery exercises that emphasize, among other things, the maintenance of cyber protection during the chaotic period of physical restoration. (Recommendation 6.14)

Clearly, some of these recommendations will require greater degrees of DOE engagement than others.

### Recommendations Directed to the Department of Homeland Security and the Department of Energy

Because emergency response and management is central to power system resilience, the committee makes several recommendations that call for collaboration between DHS and DOE.

**Recommendation 7 to DHS and DOE:** DHS and DOE should work collaboratively to improve preparation for, emergency response to, and recovery from large-area, long-duration blackouts by doing the following:

- Working with state and local authorities and electricity system operators to undertake an “all hazards” assessment of the natural hazards faced by power systems on a periodic basis (e.g., every 5 years). Local utilities should customize those assessments to their local conditions. (Recommendation 3.2)
- Developing and overseeing a process to help regional and local planners envision potential system-wide effects of long-duration loss of grid power. (Recommendation 5.3)
- Evaluating and recommending the best approach for getting critical facility managers to pre-register information about emergency power needs and available resources. (Recommendation 5.5)

- Renewing efforts to work with utilities and national, state, and local law enforcement to develop formal arrangements (such as designating selected utility personnel as “first responders”) that credential selected utility personnel to allow prompt utility access to damaged facilities across jurisdictional boundaries. (Recommendation 6.1)
- Building off of existing efforts to manufacture and stockpile flexible, high-voltage replacement transformers, in collaboration with electricity system operators and asset owners and with support from the U.S. Congress. (Recommendation 6.6)
- Developing a model for large-scale cyber restoration of electricity infrastructure. (Recommendation 6.9)

**Recommendation 8 to DHS and DOE:** With growing awareness of the electricity system as a potential target for malicious attacks using both physical and cyber means, DHS and DOE should work closely with operating utilities and other relevant stakeholders to improve physical and cyber security and resilience by doing the following:

- Working with operating utilities to sustain and enhance their monitoring and information-sharing activities to protect the grid from physical and cyber attacks. (Recommendation 3.1)
- Continuing to work with the Electricity Subsector Coordinating Council and operating utilities to enhance the sharing of cyber restoration resources (i.e., cyber mutual assistance agreements), including personnel, focusing on peer-to-peer collaboration as well as engagement with government, industry organizations, and commercial cybersecurity companies. (Recommendation 6.10)
- Working with the electricity sector and representatives of other key affected industries and sectors to continue to strengthen the bidirectional communication between federal cybersecurity programs and commercial software companies. (Recommendation 6.11)
- Redoubling efforts to reduce the vulnerability of the power system to terrorist attacks in close collaboration with FERC, NERC, and other representatives of the electric industry. (Recommendation 6.13)

### Recommendations Directed to State Offices and Regulatory Bodies

State offices and elected officials have an important role in increasing the resilience of the nation's electricity system, including through planning and regulatory decisions as well as emergency preparedness and response. Several of the committee's recommendations encourage various actors in state government to take action.

**Recommendation 9 to state offices and regulators:** Work with local utilities and relevant stakeholders to increase investment in resilience-enhancing strategies, including the following:

- State emergency planning authorities should oversee a more regular and systematic testing of backup power generation equipment at critical facilities, such as hospitals and fire stations, and ensure that public safety officials include information related to electrical safety and responses to long-duration power outages in their public briefings. (Recommendation 5.1)
- Utility regulators should work closely with operating utilities to assess their current interconnection standards as applicable to DERs, consider the costs of requiring new installations to use enhanced inverters, and determine the appropriate policy for promoting islanding and other related capabilities. (Recommendation 5.7)
- State legislatures and utility regulatory bodies should explore economic, ratemaking, and other regulatory options for facilitating the development of private microgrids that provide resilience benefits. (Recommendation 5.9)
- Utility regulators and non-governmental entities should undertake studies to develop guidance on how best to compensate the owners of distributed generation resources who are prepared to commit a portion of their distributed generation capacity to serve islanded feeders in the event of large outages of long duration. Additionally, the National Association of Regulatory Utility Commissioners (NARUC) should establish a working group to advise members on the issues they will likely have to address. (Recommendation 5.11)

**Recommendations Directed to the National Association of Regulatory Utility Commissioners and Federal Organizations**

NARUC is uniquely capable of convening and disseminating information to regulators from diverse states while providing a single point of contact with federal agencies.

**Recommendation 10 to NARUC and federal organizations:** The committee recommends that NARUC work with DHS and DOE as follows:

- Develop model guidance on how state regulators, utilities, and broader communities (where appropriate) might consider the equity and social implications of choices in the level and allocation of investments. (Recommendation 5.2)
- Develop guidance to state regulators and utilities on (1) selective restoration options as they become available,

(2) the factors that should be considered in making choices of which loads to serve, and (3) model recommendations that states and utilities can build upon and adapt to local circumstances. (Recommendation 5.4)

- Undertake studies of the technical, economic, and regulatory changes necessary to allow development and operation of privately owned microgrids that serve multiple parties and/or cross public rights-of-way. (Recommendation 5.8)

**Recommendation Directed to the Federal Energy Regulatory Commission and the North American Energy Standards Board**

The growing interdependence of natural gas and electricity infrastructures requires systematic study and targeted efforts to improve coordination and planning across the two industries.

**Recommendation 11 to FERC and the North American Energy Standards Board:** FERC, which has regulatory authority over both natural gas and electricity systems, should address the growing risk of interdependent infrastructure by doing the following:

- Working with the North American Energy Standards Board and industry stakeholders to improve awareness, communications, coordination, and planning between the natural gas and electric industries. (Recommendation 4.7)

**Recommendation Directed to the North American Electric Reliability Corporation**

Following large-scale outages, detailed investigations are essential to support the learning phase of resilience. NERC, with authority delegated from FERC, has conducted several such investigations.

**Recommendation 12 to NERC:** Review and improve incident investigation processes to better learn from outages that happen and broadly disseminate findings and best practices by doing the following:

- Engaging relevant regional and state-level organizations to improve the investigation process of large-scale losses of power, drawing lessons from the National Transportation Safety Board and others, with the objective of disseminating lessons across geographical and jurisdictional boundaries. (Recommendation 6.15)

CONCLUSIONS

141

REFERENCES

Fischhoff, B., P. Slovic, and S. Lichtenstein. 1978. Fault trees: Sensitivity of estimated failure probabilities to problem representation. *Journal of Experimental Psychology: Human Perception and Performance* 4: 342–355.

Kahneman, D. 2011. *Thinking Fast and Slow*. New York: Farrar, Straus, and Giroux.

Kingdon, J.W. 1984. *Agendas, Alternatives, and Public Policies*. Boston: Little, Brown, and Company.

Lindblom, C.E. 1959. The science of muddling through. *Public Administration Review* 19(2): 79–88.





# Appendix A

## Statement of Task

An ad hoc National Research Council (NRC) committee will address technical, policy and institutional factors that might affect how modern technology can be implemented in the evolution of electric transmission and distribution (T&D) in the United States, and recommend strategies and priorities for how the nation can move to a more reliable and resilient T&D system. The committee will consider how existing and emerging technological options, including greater reliance on distributed power generation, could impact the reliability, robustness, and the ability to recover from disruptions to the electrical T&D system or systems. The study will identify barriers to implementing technology pathways for improving T&D reliability, key priorities and opportunities including, where necessary, those for research, development and demonstration (RD&D), the federal role, and strategies and actions that could lead to a more reliable and resilient T&D system. As part of this study the committee may do the following:

1. Review recent studies and analysis of the current and projected status of the nation's electric T&D system including any that identify significant technological concerns over vulnerability, reliability, and resilience;
2. Assess factors affecting future requirements and trends for the nation's T&D infrastructure including such issues as the need for new capacity, replacement needs, siting issues, vulnerability to external threats and the need for security, whether physical or cyber, the alignment of costs and benefits, the effects of interconnectedness among regional networks, and others identified by the committee;
3. Evaluate the role existing and emerging technological options, especially of renewable and distributed generation technologies, can play in creating or addressing concerns identified by the committee and that can lead to enhanced reliability and resilience;
4. Consider how regional differences both in terms of the physical setting and the utility structure may impact solutions to improving resilience;
5. Review federal, state, industry, and academic R&D programs, as well as any demonstration and/or deployment efforts, focused on technologies for the T&D system that are aimed at improving its capacity, reliability, resilience, flexibility, and any other attributes aimed at enhancing the robustness of the nation's electric power T&D system;
6. Identify non-technological barriers (including those related to regulatory, ownership, and financial issues) to implementation of new and/or expanded technology to improve the stability, reliability, and resilience of electric T&D;
7. Suggest strategies, key opportunities and priorities, and actions for implementation of the identified technology pathways for the T&D system, which could include RD&D, policies, incentives, standards, and others the committee finds are necessary; and
8. Address the federal role, especially of DOE, in addressing the technical, policy, and institutional issues for a transformation of the T&D system to one with increased robustness and resilience.

# Appendix B

## Committee Biographies

M. GRANGER MORGAN, *Chair*, is Hamerschlag University Professor of Engineering; professor, Department of Engineering and Public Policy (where he served for 38 years as the founding department head) and Electrical and Computer Engineering at Carnegie Mellon University. He also holds an appointment in the H. John Heinz III College of Public Policy and Management. He is a fellow of the Institute of Electrical and Electronics Engineers (IEEE), the American Association for the Advancement of Science, and the Society for Risk Analysis. His research addresses problems in science, technology, and public policy with a particular focus on energy, environmental systems, climate change, and risk analysis. Much of his work has involved the development and demonstration of methods to characterize and treat uncertainty in quantitative policy analysis. At Carnegie Mellon, he co-directs (with Inês Azevedo) the Center for Climate and Energy Decision Making and (with Jay Apt) the Electricity Industry Center. He is a member of the National Academy of Sciences, serves on several committees for the National Academies of Sciences, Engineering, and Medicine, and is a member of several domestic and international advisory committees for organizations addressing issues involving electric power, other energy issues, and the management of risks to health safety and the environment. He holds a B.A. from Harvard College (1963) where he concentrated in physics, an M.S. in astronomy and space science from Cornell University (1965), and a Ph.D. from the Department of Applied Physics and Information Sciences at the University of California, San Diego (1969).

DIONYSIOS ALIPRANTIS is an associate professor of electrical and computer engineering at Purdue University. Dionysios obtained his Ph.D. from Purdue University in 2003 and his Diploma in electrical and computer engineering from the National Technical University of Athens, Greece, in 1999. Prior to joining Purdue, he was an assistant professor of electrical and computer engineering at Iowa State University. His research interests include electromagnetic energy conversion and electric machinery, power electronics, and

power systems analysis. More recently, his work has focused on technologies that enable the integration of renewable energy sources in the electric power system and the electrification of transportation. He is currently serving as an associate editor for the *IEEE Transactions on Energy Conversion*.

ANJAN BOSE is Regents Professor and Distinguished Professor of Electric Power Engineering at Washington State University. He has 50 years of experience in industry, academia, and government, as an engineer, educator, and administrator. He is also the site director of the National Science Foundation (NSF)-sponsored Power System Engineering Research Center. He served as the dean of the College of Engineering and Architecture (1998–2005) and as the director of the School of Electrical Engineering and Computer Science (1993–1998). Prior to Washington State University, he taught at Arizona State University (1981–1993) and worked in the Energy Management Systems Division of Control Data Corporation (now Siemens), where he developed power grid control software. He is a member of the U.S. National Academy of Engineering and the Indian National Academy of Engineering. A fellow of the IEEE, he was the recipient of the Outstanding Power Engineering Educator Award (1994), the Third Millennium Medal (2000), and the IEEE's Herman Halperin Electric Transmission and Distribution Award (2006). He has been recognized as a distinguished alumnus of the Indian Institute of Technology, Kharagpur (2005) and the College of Engineering at Iowa State University (1993). During 2011–2013, Bose served as senior advisor to the Department of Energy (DOE) coordinating priorities for the next-generation grid.

W. TERRY BOSTON is the former chief executive officer of PJM Interconnection, the largest power grid in North America and the largest electricity market in the world. Boston is past president of the Association of Edison Illuminating Companies and past president of GO 15, the association of the world's largest power grid operators. He also served as a U.S. vice president of the International Council of Large

Electric Systems and is a past chair of the North American Transmission Forum. He also was one of the eight industry experts selected to direct the North American Electric Reliability Corporation investigation of the August 2003 Northeast blackout. In 2011, Boston was honored with the Leadership in Power award from the IEEE Power and Energy Society. He also was chosen by *Intelligent Utilities* as one of the Top 11 Industry Movers and Shakers and led PJM to win Platts Global Energy Awards in Industry Leadership in 2010, Excellence in Electricity in 2012, and Lifetime Achievement Award in 2015. Boston is a member of the National Academy of Engineering. He received a B.S. in engineering from the Tennessee Technological University and an M.S. in engineering administration from the University of Tennessee.

ALLISON CLEMENTS is the president of goodgrid, LLC, based in Salt Lake City, Utah. She is the former director of the Sustainable Federal Energy Regulatory Commission (FERC) Project at Natural Resources Defense Council (NRDC). The Project represents a coalition of clean energy-focused advocacy organizations at FERC and at the independent system operator/regional transmission organization level in pursuit of a clean, reliable, and affordable electric system. Prior to joining the FERC Project, Clements spent 3 years as NRDC's corporate counsel while maintaining a policy practice in renewable energy deployment. Before joining NRDC, she worked as a project finance attorney at Chadbourne & Parke, LLP, as well as an energy regulatory attorney at Troutman Sanders, LLP. Clements is a 2015 Presidio Institute Cross-Sector Leadership Fellow, co-directed the Yale Law School and School of Forestry Environmental Protection Clinic (2013–2014), acted as co-chair of the Bipartisan Policy Center's Electric Grid Initiative (2011–2013), and served as a director and treasurer of the Healthy Building Network (2008–2014). She holds a B.S. in environmental policy from the University of Michigan and a J.D., with honors, from the George Washington University Law School.

JEFFERY DAGLE has been an electrical engineer at the Pacific Northwest National Laboratory since 1989. He currently manages several projects in the areas of transmission reliability and security, including the North American SynchroPhasor Initiative and cybersecurity reviews for the DOE Smart Grid Investment Grants and Smart Grid Demonstration Projects. He is a senior member of the IEEE and the National Society of Professional Engineers. He received the 2001 Tri-City Engineer of the Year award by the Washington Society of Professional Engineers, led the data requests and management task for the U.S.-Canada Power System Outage Task Force investigation of the August 14, 2003, blackout, supported the DOE Infrastructure Security and Energy Restoration Division with on-site assessments in New Orleans following Hurricane Katrina in fall 2005, and is the recipient of multiple patents including a Federal Laboratory Consortium Award in 2007 and an R&D 100 Award in 2008 for the

Grid Friendly™ Appliance Controller technology. Dagle was a member of a National Infrastructure Advisory Council study group formed in 2010 to establish critical infrastructure resilience goals. He received B.S. and M.S. degrees in electrical engineering from Washington State University in 1989 and 1994, respectively.

PAUL DE MARTINI is the managing director at Newport Consulting. He has more than 35 years of experience in the power industry. He is a thought leader and expert in the global electricity industry, providing guidance to utilities, policy makers, and new entrants. Previously, De Martini held several executive positions focused on strategy, policy, and technology development, including chief technology and strategy officer for Cisco's Energy Networks Business and vice president of Advanced Technology at Southern California Edison. De Martini has an M.B.A. from the University of Southern California and a B.S. in applied economics from the University of San Francisco. He is a visiting scholar at the California Institute of Technology.

JEANNE FOX is an adjunct professor at Columbia University's School of International and Public Affairs and at Rutgers University School of Arts and Sciences. She served as a commissioner of the New Jersey Board of Public Utilities from January 2002 until September 2014 and was its president and a member of the Governor's cabinet from January 2002 to January 2010. The New Jersey Board of Public Utilities has regulatory jurisdiction over telephone, electric, gas, water, wastewater, and cable television companies and works to ensure that consumers have proper service at reasonable rates. Commissioner Fox is currently a member of the National Petroleum Council and its Emergency Preparedness Committee, Carnegie Mellon University's Advisory Board for its Center for Climate Energy Decision Making, Rutgers University's Energy Institute Advisory Board, and GRID Alternatives Tri-State Board of Directors. Fox was active with the National Association of Regulatory Utility Commissioners as a member of the Board of Directors (2003–2014), Subcommittee on Education and Research, Subcommittee on Utility Market Access, Committee on Energy Resources and Environment (chair, vice chair), and Committee on Critical Infrastructure (vice chair). She is currently a member of the National Association of Regulatory Utility Commissioners' Emeritus. Fox served as Region 2 administrator of the United States Environmental Protection Agency (1994–2001) and as commissioner and deputy commissioner of the New Jersey Department of Environmental Protection and Energy (1991–1994). Starting at the Board of Public Utilities in 1981 as a regulatory officer, she was promoted to Solid Waste Division deputy director (1985), Water Division director (1987), and chief of staff (1990–1991). In 2001, Fox was a visiting distinguished lecturer at Rutgers University's Bloustein School of Planning and Public Policy and at Princeton University's Woodrow Wilson School of Public and International Affairs.

(2001–2002, 2016–2017). Fox is currently president of the associate alumnae of Douglass College and a Rutgers University trustee emerita. She is a member of the Rutgers Hall of Distinguished Alumni Award (1997) and the Douglass Society (1993) and a recipient of the Rutgers Alumni Federation Alumni Meritorious Service Award (1991) and the Loyal Sons and Daughters of Rutgers Award (2012). Fox graduated cum laude from Douglass College, Rutgers University, and received a J.D. from the Rutgers University School of Law, Camden.

ELSA GARMIRE is the former Sydney E. Junkins Professor at Thayer School of Engineering, Dartmouth College. She received her A.B. at Harvard and her Ph.D. at M.I.T., both in physics. After postdoctoral work at Caltech, she spent 20 years at the University of Southern California, where she was eventually named William Hogue Professor of Electrical Engineering and director of the Center for Laser Studies. She came to Dartmouth in 1995 as dean of Thayer School of Engineering. In her technical field of quantum electronics, lasers, and optics, she has authored more than 250 journal papers, obtained nine patents, and been on the editorial board of five technical journals. She has supervised 30 Ph.D. theses and 14 M.S. theses. Garmire is a member of the National Academy of Engineering, on whose Governing Council she has served, and the American Academy of Arts and Sciences. She is a fellow of IEEE, the American Physical Society, and the Optical Society of America, of which she was president in 1993. In 1994, she received the Society of Women Engineers Achievement Award. Garmire has been a Fulbright senior lecturer in fiber optics and a visiting faculty member in Japan, Australia, Germany, and China. She chaired the NSF Advisory Committee on Emerging Technology and served on both the NSF Advisory Committee on Engineering and the Air Force Science Advisory Board. With her electrical engineering background and fiber-optics expertise, she has followed the growing challenges to the nation's energy infrastructure, with particular interest in the electric grid.

RONALD E. KEYS, an independent consultant, retired from the Air Force in November 2007 after completing a career of more than 40 years. His last assignment was as Commander, Air Combat Command, the Air Force's largest major command, consisting of more than 1,200 aircraft, 27 wings, 17 bases, and 200 operating locations worldwide with 105,000 personnel. General Keys holds a B.S. from Kansas State University and an M.B.A. from Golden Gate University. General Keys is a command pilot with more than 4,000 flying hours in fighter aircraft, including more than 300 hours of combat time. No stranger to energy challenges, General Keys first faced them operationally as a young Air Force Captain, piloting F-4s during the fuel embargo of the 1970s. Later, as director of operations for European Command, fuel and logistic supply provisioning were critical

decisions during humanitarian, rescue, and combat operations across European Command's area of responsibility including the Balkans and deep into Africa. As Commander of Allied Air Forces Southern Europe and Commander of the U.S. 16th Air Force, similar hard choices had to be made in supporting OPERATION NORTHERN WATCH in Iraq as well as for combat air patrols and resupply in the Balkans. Later, as the director of all Air Force Air, Space, and Cyber mission areas as well as operational requirements in the early 2000s, he saw the impact of energy choices on budget planning and execution as well as in training and supporting operational plans in Iraq and Afghanistan. Finally, at Air Combat Command, he faced the total challenge of organizing, training, and equipping forces at home and deployed to balance mission effectiveness with crucial energy efficiency, security, and resilience. Continuing after retirement, he has advised the U.S. Air Force on energy security strategy planning and acted as a subject matter expert during analysis of energy impacts and trade-offs in "futures" war games. As a Bipartisan Center senior advisor, he served as a technical advisor on the "Cyber Shockwave" exercise based on cyber and physical grid and internet attacks. He is a member of The Center for Climate and Security's Advisory Board as well as their Climate and Security Working Group focused on developing policy options and encouraging dialogue and education. As chairman of the CNA Military Advisory Board on Department of Defense Energy Security and Climate Change, he is intimately familiar with the relationship of energy, military, economic, and national security and has contributed to a number of energy and climate reports, most recently concerning the vulnerability and resilience of the electric grid.

MARK McGRANAGHAN is vice president of distribution and energy utilization for the Electric Power Research Institute (EPRI). This research area is leading the development of the next generation integrated grid while continuing to develop new innovations for designing, maintaining, and improving the existing grid. This includes research to define and develop the information and communication infrastructure that will support the integrated grid. He has been involved in resiliency research at EPRI at both the transmission and distribution levels. McGranaghan has more than 35 years of experience in the industry. He has authored more than 70 technical papers and articles on topics ranging from power quality to insulation coordination of extra-high-voltage systems. He is an IEEE fellow and, in 2014, received the Charles Proteus Steinmetz award for his expertise and dedication to power engineering standards development. He has recently been one of the industry leaders developing the standards and platforms to support the next-generation smart grid for integration of widespread distributed resources. He is a member of the executive committee of the CIGRE U.S. National Committee, vice chairman of the CIRED U.S. National Committee, and a member



of the International Electrotechnical Commission Advisory Committee on Electricity Transmission and Distribution. McGranaghan has taught courses and seminars around the world to help support collaboration in the power industry. He is a co-author of the book *Electrical Power Systems Quality*, now in its third edition. McGranaghan has a B.S.E.E. from the University of Toledo and an M.B.A. from the University of Pittsburgh. In 2015, he received the Outstanding Alumni Award from the University of Toledo College of Engineering and Computer Science.

CRAIG MILLER currently serves full time as the National Rural Electric Cooperative Association's chief scientist. Miller is a technologist with extensive background in the physical sciences, information technology, and systems engineering. He has developed new technology and cutting-edge systems for more than 30 years, within and for both start-up and established corporations. His particular strength is the conceptualization, tuning, and positioning of new technology products. More than 2,000 companies in the United States use systems or technology he has architected or developed. Miller's many accomplishments deserve mention: participating in seven start-ups; serving as SAIC's chief scientist (during which time he was granted the "Heroic Achievement in Information Technology" award from the Smithsonian Institution); and a wide experience in technical and financial media as a key investor relations expert, technologist, inventor, and analyst on behalf of diverse companies such as Proxicom, GridPoint, DiData, and Aguru Images, a high-end digital imaging company that he started. More recently, Miller has achieved a national reputation in the advanced smart grid and cybersecurity arenas.

THOMAS J. OVERBYE is a Texas A&M Engineering Experiment Station Distinguished Research Professor in the Electrical and Computer Engineering Department at Texas A&M University. Formerly, he was the Fox Family Professor of Electrical and Computer Engineering at the University of Illinois, Urbana-Champaign, where he has taught since 1991. He received his B.S., M.S., and Ph.D. in electrical engineering from the University of Wisconsin, Madison and is a member of the National Academy of Engineering. His current research interests include electric power system analysis, visualization, dynamics, cybersecurity, and modeling of power system geomagnetic disturbances. Overbye is the original developer of the PowerWorld Simulator, an innovative computer program for power system analysis, education, and visualization; a co-founder of PowerWorld Corporation; and an author of *Power System Analysis and Design*. He was the recipient of the IEEE/Power and Energy Society Walter Fee Outstanding Young Engineer Award in 1993 and the IEEE/Power and Energy Society Outstanding Power Engineering Educator Award in 2011, and he participated in the 2003 DOE/North American Electric Reliability Corporation Blackout investigation.

WILLIAM H. SANDERS is Donald Biggar Willett Professor of Engineering and the head of the Department of Electrical and Computer Engineering at the University of Illinois, Urbana-Champaign. Dr. Sanders's research interests include secure and dependable computing and security and dependability metrics and evaluation, with a focus on critical infrastructures. He has published more than 270 technical papers in those areas. He served as the director and principal investigator of the DOE/Department of Homeland Security Trustworthy Cyber Infrastructure for the Power Grid Center, which is at the forefront of national efforts to make the U.S. power grid smart and resilient. He is also co-developer of three tools for assessing computer-based systems: METASAN, UltraSAN, and Möbius. Möbius and UltraSAN have been distributed widely to industry and academia; more than 1,700 licenses for the tools have been issued to universities, companies, and NASA for evaluating the performance, dependability, and security of a variety of systems. He is also a co-developer of the Network Access Policy Tool for assessing the security of networked systems; it is available commercially under the name NP-View from the start-up company Network Perception, which was cofounded by Dr. Sanders.

RICHARD E. SCHULER is a professor of economics (College of Arts and Sciences), a professor emeritus of civil and environmental engineering (College of Engineering), and a graduate school professor at Cornell University. Schuler served on the executive committee of the NSF-supported, multi-university Institute for Civil Infrastructure Systems. Previous administrative positions at Cornell have included director of the Waste Management Institute and the New York State Solid Waste Combustion Institutes (1987–1993), as associate director of the Center for the Environment (1989–1993), and director of Cornell's Institute for Public Affairs (1995–2001), a university-wide multidisciplinary program offering the M.P.A. degree. He has served on the Board of Trustees of Cornell University (1993–1997). Schuler's industrial and government experience include engineer and manager with the Pennsylvania Power and Light Company (1959–1968), energy economist with Battelle Memorial Institute (1968–1969), and public service commissioner and deputy chairman for New York State (1981–1983). He has been a consultant to numerous government agencies and industries on pricing, management, and environmental issues and to the World Bank on energy and infrastructure investment programs. From its inception in 1999 until April 2012, he was a founding board member of the New York Independent System Operator that is responsible for operating the electric transmission grid reliably in New York while overseeing an efficient power market. During his tenure he chaired the New York Independent System Operator board's market performance, reliability and markets, and its governance committees, and from 2008–2010 he was the board's lead director. Schuler's degrees include a B.E. in electrical

engineering, Yale, 1959; an M.B.A., Lehigh, 1969; and a Ph.D. in economics, Brown, 1972. He has been a registered professional engineer in Pennsylvania since 1963.

SUSAN TIERNEY is a senior advisor at Analysis Group and is an expert on energy economics, regulation, and policy, particularly in the electric and gas industries. She has consulted to businesses, governments, tribes, non-profit organizations, foundations, and other organizations on energy markets, economic and environmental regulation and strategy, and energy policy. She has participated as an expert in civil litigation cases, in regulatory proceedings before state and federal agencies, on a variety of boards and commissions, and on National Academies' committees. Previously, she served as the assistant secretary for policy at DOE. She was the secretary for environmental affairs in Massachusetts, commissioner at the Massachusetts Department of Public Utilities, chairman of the Board of the Massachusetts Water Resources Authority, and executive director of the Massachusetts Energy Facilities Siting Council. She chairs DOE's Electricity Advisory Committee as well as the External Advisory Board of the National Renewable Energy Laboratory, and she previously served on the Secretary of Energy Advisory Board. She is a director of the World Resources

Institute, Resources for the Future, and other boards. She has published widely, frequently speaks at industry conferences, and has lectured at many leading universities. Tierney received her Ph.D. and M.A. in regional planning from Cornell University.

DAVID G. VICTOR is director of the Laboratory on International Law and Regulation and a professor at the School of Global Policy and Strategy at the University of California, San Diego, where he also co-leads the university's Deep Decarbonization Initiative. His research focuses on how regulatory law affects the environment, technology choices, industrial structure, and the operation of major energy markets. Prior to joining the University of California, San Diego, Victor served as director of the Program on Energy and Sustainable Development at Stanford University where he was also a professor at the law school. He is a member of the Board of Directors of EPRI, on the advisory council for the Institute of Nuclear Power Plant Operators, and chairman of the Community Engagement Panel that is helping to guide the decommissioning of Units 2 and 3 at the San Onofre Nuclear Generating Station. He has contributed to numerous publications on topics such as energy market innovations and electric power market reform.



# Appendix C

## Disclosure of Conflicts of Interest

The conflict of interest policy of the National Academies of Sciences, Engineering, and Medicine ([www.nationalacademies.org/coi](http://www.nationalacademies.org/coi)) prohibits the appointment of an individual to a committee like the one that authored this Consensus Study Report if the individual has a conflict of interest that is relevant to the task to be performed. An exception to this prohibition is permitted only if the National Academies determine that the conflict is unavoidable and the conflict is promptly and publicly disclosed.

When the committee that authored this report was established, a determination of whether there was a conflict of interest was made for each committee member given the individual's circumstances and the task being undertaken by the committee. A determination that an individual has a conflict of interest is not an assessment of that individual's actual behavior, character, or ability to act objectively despite the conflicting interest.

Mr. Paul De Martini was determined to have a conflict of interest because he is the managing director at Newport Consulting. Dr. Susan Tierney was determined to have a conflict of interest because she is the senior advisor at Analysis Group and also performs consulting work.

In each case, the National Academies determined that the experience and expertise of the individual was needed for the committee to accomplish the task for which it was established. The National Academies could not find another available individual with the equivalent experience and expertise who did not have a conflict of interest. Therefore, the National Academies concluded that the conflict was unavoidable and publicly disclosed it through the National Academies' Current Projects System ([www8.nationalacademies.org/cp](http://www8.nationalacademies.org/cp)).

# Appendix D

## Presentations and Committee Meetings

### FIRST COMMITTEE MEETING MARCH 2–3, 2016 WASHINGTON, D.C.

FERC Activities in the Office of Electric Reliability  
*Michael Bardee, Federal Energy Regulatory Commission, Office of Electric Reliability*

EPRI Activities in Electricity Sector Modernization  
*Mark McGranaghan, Electric Power Research Institute*

NERC and APPA Activities in Critical Infrastructure Protection  
*Nathan Mitchell, American Public Power Association*

DOE Office of Electricity Perspective on NAS Committee Task  
*Patricia Hoffman, Department of Energy, Office of Electricity Delivery and Energy Reliability*

### SECOND COMMITTEE MEETING MAY 11–12, 2016 WASHINGTON, D.C.

Overview of Relevant DOE Activities and Needs  
*Gilbert Bindewald, Department of Energy, Office of Electricity Delivery and Energy Reliability*

Improving Resilience of Transformers  
*Richard Boyd, Siemens*  
*James McIver, Siemens*

Resilience Through Relays, Sensors, and Components  
*Gregory Zweigle, Schweitzer Engineering Laboratories*

Resilience through Automation and Trade-offs with Cybersecurity  
*Steven Kunsman, ABB*

Cybersecurity and Activities in NERC and E-ISAC  
*Tim Roxey, Electricity Information Sharing and Analysis Center*

### THIRD COMMITTEE MEETING JULY 11–12, 2016 WASHINGTON, D.C.

Panel on State Regulatory Commissions and Resilience  
*Paul Centolella, Paul Centolella and Associates*  
*David Littell, Regulatory Assistance Project*  
*Kris Mayes, Utility of the Future Center*  
*Audrey Zibelman, New York State Public Service Commission*

Extreme Weather Events  
*Tom Karl, National Oceanic and Atmospheric Administration's National Centers for Environmental Information*  
*Jim Kossin, National Oceanic and Atmospheric Administration's National Centers for Environmental Information*  
*Ken Kunkel, National Oceanic and Atmospheric Administration's National Centers for Environmental Information*  
*Mike Squires, National Oceanic and Atmospheric Administration's National Centers for Environmental Information*

Trends in Battery Storage  
*Jay Whitacre, Carnegie Mellon University*

### FOURTH COMMITTEE MEETING SEPTEMBER 29–30, 2016 WASHINGTON, D.C.

Utility Perspectives on Resilience  
*Joe Svachula, Commonwealth Edison*  
*Ralph LaRossa, Public Service Enterprise Group*  
*William Ball, Southern Company*  
*Erik Takayesu, Southern California Edison*

Distribution Resilience with High Automation  
*Jim Glass, Chattanooga Electric Power Board*

*APPENDIX D*

151

Briefing on RAND Resilience Report  
*Henry Willis, RAND Corporation*  
Industry-wide Trends in Resilience  
*David Owens, Edison Electric Institute*

**FIFTH COMMITTEE MEETING  
NOVEMBER 2–3, 2016  
WASHINGTON, D.C.**

No open session presentations were held at this meeting.

**SIXTH COMMITTEE MEETING  
FEBRUARY 15–16, 2017  
WASHINGTON, D.C.**

No open session presentations were held at this meeting.

# Appendix E

## Examples of Large Outages

### **NORTHEAST BLACKOUT AFFECTING UNITED STATES AND SOUTHEAST CANADA (AUGUST 13, 2003)**

#### **Pre-Event**

Due to the minimal amount of warning time before this event, no significant preparations were taken.

#### **Event**

High electricity demand in central Ohio combined with scheduled maintenance of several generators resulted in low voltage around the Cleveland-Akron area. Computer and alarm systems failed to warn operators due to software bugs in both the power company's and regulating authority's computer systems. Three 345 kV lines feeding central Ohio tripped due to contact with trees. Cascading failures resulted throughout the region as lower-voltage lines attempted and failed to take on the redistributed load from tripped lines. The blackout affected at least 50,000,000 customers, caused a loss of 70,000 MW, cost \$4–10 billion, and contributed to 11 deaths.

#### **Recovery**

Most areas were restored to full power within hours, but some areas in the United States were without power for 4 days. Parts of Ontario experienced rotating blackouts for up to 2 weeks. Physical damage was limited, making recovery much faster than other types of events.

#### **Lessons Learned**

Improvements in system protection to slow or limit cascading failures should be made. Improvements in operator training, emergency response plans, communication between reliability coordinators and utilities, and sensor usage should

also be made. Managing and pruning of vegetation and vegetation-caused bulk incidents should be reported to the North American Electric Reliability Corporation (NERC) and regional reliability coordinators (NERC, 2004).

### **WEST COAST BLACKOUT (AUGUST 10, 1996)**

#### **Pre-Event**

Due to the minimal amount of warning time before this event, no significant preparations were taken.

#### **Event**

Heavy loading on 500 kV transmission lines and the western interconnect system was caused by good hydro conditions in the northwest region and high demand in California resulting from high summer temperatures. The 500 kV Big Eddy-Ostrander line arced to a tree, followed by four more 500 kV lines over 100 minutes. Several smaller lines also arced and closed. Systems protections removed 1,180 MW of generation from the system, creating an unstable power oscillation and ultimately causing islanding of the Western Electricity Coordinating Council into four distinct islands: Island 1, Alberta, Canada; Island 2, Colorado to British Columbia; Island 3, Central to Northern California; and Island 4, Southern California to New Mexico to Northern Mexico. The outage affected approximately 7,500,000 customers and caused a loss of 33,024 MW.

#### **Recovery**

Physical damage was limited, making recovery much faster than other types of events. Islands 1 and 2 had power restored within 2 hours. Island 3 was restored within 9 hours. Island 4 was restored within 6 hours.

## APPENDIX E

**Lessons Learned**

Limiting certain high-voltage lines would prevent cascading failures. Insuring coordination between power producers and transmission operators is imperative (NERC, 2002).

**GEOMAGNETIC DISTURBANCE AFFECTING EASTERN CANADA (MARCH 13, 1989)****Pre-Event**

Due to the small amount of warning time before this event, no significant preparations were taken. However, forecasts for solar storm events may enable preparation in the future.

**Event**

At 2:45 a.m., a solar magnetic storm resulting from a solar flare tripped five lines in Eastern Canada by inducing a quasi-direct current. The land surrounding the Hudson Bay rests on an igneous rock shield, making the region more susceptible to ground-induced currents that result from solar storms. Higher latitudes also determine a location's magnetic storm vulnerability. The outage affected approximately 6,000,000 customers and caused a loss of 19,400 MW.

**Recovery**

Forty-eight percent of power was restored after 5 hours. Eighty-three percent of power was restored after 9 hours. Some strategic equipment and two major step-up transformers were damaged and required repair due to overvoltage.

**Lessons Learned**

NERC urged the National Oceanic and Atmospheric Administration for the capabilities and coordination for at least 1 hour of notice of solar storms. Forecasting remains less precise compared to meteorological events but still has potential to give minutes to hours of warning to grid operators for the approach of strong solar storms. Current standards require systems to withstand benchmark geomagnetic disturbance events, particularly to prevent high-voltage transformers from overheating (NERC, 1989).

**ICE STORM AFFECTING SOUTHERN CANADA AND THE NORTHEAST UNITED STATES (JANUARY 10, 1998)****Pre-Event**

The severity of the ice storm was poorly predicted since icing conditions depend critically on the vertical atmospheric temperature profile. As a result, officials did not make any significant preparations for this event.

**Event**

During a series of severe ice storms beginning on January 5, heavy ice and snow loads caused the destruction of trees and high-voltage towers. Thirty thousand wooden utility poles collapsed, leaving millions without power. Two major generating stations were disconnected from the rest of the grid due to line tripping, causing the area to blackout. The bulk transmission grid remained mostly intact, keeping the outage from spreading too far outside of the Québec area. The outage affected 2,800,000 customers and caused a loss of 18,500 MW.

**Recovery**

Hundreds of utility crews from outside the area were brought in, along with 16,000 Canadian military personnel, making this the largest deployment of Canadian military since the Korean War. American military also assisted in recovery efforts. Northern New York and New England had their power returned within 3 weeks. Québec had its power back online within 4 weeks.

**Lessons Learned**

Disruptions of telephone, cellular, and fiber-optic cables made communication difficult. The most reliable means of communications were found to be the utility-owned and operated microwave and mobile radio systems. More accurate temperature profiling and precautions around temperatures where ice storms are possible would be beneficial for preparing for any outage that results from these types of storms. Building towers and lines to withstand greater weights from icing would also result in greater resilience (NERC, 2001).

**HURRICANE SANDY AFFECTING THE NORTHEAST UNITED STATES (OCTOBER 29, 2012)****Pre-Event**

Unlike unexpected cascading failures or solar storms, hurricanes typically offer days of warning before outages occur. In the days leading up to landfall, extensive communication was made between utilities and generating facilities to prepare for abnormal operation, including preparing black-start units with enough fuel for emergency use. Additional field operation crews were made available for response. Sandbags and other barriers were put around vulnerable substations. In the minutes and hours leading up to outages, flood-prone areas were de-energized.

**Event**

Superstorm Sandy made landfall over New Jersey, New York, and the northern mid-Atlantic with wind speeds of

about 80 mph at landfall and a storm surge that flooded low-lying assets, causing more than 260 transmission trips and loss of roughly 20,000 MW of generation capacity. High winds and flooding were the major causes of outages, with some snow and icing contributing as well. More than 5,770,000 customers were affected.

### Recovery

Ninety-five percent of customers' power was restored between November 1, 2012, and November 9, 2012.

### Lessons Learned

Pre-staging equipment for recovery and de-energizing facilities in flood-prone areas can mitigate losses and hasten recovery. Implementing flood-protected facilities that include water-tight doors and barricades would prevent some stations from tripping (NERC, 2014).

### REFERENCES

- NERC (North American Electric Reliability Corporation). 1989. *March 13, 1989 Geomagnetic Disturbance*. <http://www.nerc.com/files/1989-Quebec-Disturbance.pdf>.
- NERC. 2001. *1998 System Disturbances: Review of Selected Electric System Disturbances in North America*. <http://www.nerc.com/pa/rrm/ea/System%20Disturbance%20Reports%20DL/1998SystemDisturbance.pdf>.
- NERC. 2002. *Review of Selected 1996 Electric System Disturbances in North America*. <http://www.nerc.com/pa/rrm/ea/System%20Disturbance%20Reports%20DL/1996SystemDisturbance.pdf>.
- NERC. 2004. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* [http://www.nerc.com/docs/blackout/NERC\\_Final\\_Blackout\\_Report\\_07\\_13\\_04.pdf](http://www.nerc.com/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf).
- NERC. 2014. *Hurricane Sandy Event Analysis Report*. [http://www.nerc.com/pa/rrm/ea/Oct2012HurricaneSandyEventAnalysisRptDL/Hurricane\\_Sandy\\_EAR\\_20140312\\_Final.pdf](http://www.nerc.com/pa/rrm/ea/Oct2012HurricaneSandyEventAnalysisRptDL/Hurricane_Sandy_EAR_20140312_Final.pdf).



# Appendix F

## Acronyms

AC	alternating current
AMI	advanced metering infrastructure
APS	Arizona Public Services
BPA	Bonneville Power Administration
C&I	commercial and industrial
CAISO	California Independent System Operator
CAP	Civil Air Patrol
CHP	combined heat and power
CIP	critical infrastructure protection
DC	direct current
DER	distributed energy resource
DES	distributed energy storage
DG	distributed generation
DHS	Department of Homeland Security
DMS	distribution management system
DOD	Department of Defense
DOE	Department of Energy
DR	demand response
DSO	distribution system operator
E-ISAC	Electricity Information Sharing and Analysis Center
EEI	Edison Electric Institute
EIA	Energy Information Administration
EIM	Energy Imbalance Market
EMP	electromagnetic pulse
EMS	energy management system
EPAct	Energy Policy Act
EPB	Electric Power Board
EPRI	Electric Power Research Institute
ERCOT	Electric Reliability Council of Texas
ERD	entity relationship diagram
FAA	Federal Aviation Administration
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FPA	Federal Power Act

GMD	geomagnetic disturbance
GMLC	Grid Modernization Laboratory Consortium
GPS	global positioning satellites
GW	gigawatt
ICC	Illinois Commerce Commission
ICS	industrial control system
IEEE	Institute of Electrical and Electronics Engineers
IPCC	Intergovernmental Panel on Climate Change
ISO	independent system operator
JCESR	Joint Center for Energy Storage Research
LOLP	loss of load probability
LPT	large power transformer
MAA	mutual assistance agreement
MW	megawatt
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NPS	National Preparedness System
NRC	National Research Council
NRCC	National Response Coordination Center
NRDC	National Resources Defense Council
NSF	National Science Foundation
OMS	outage management system
OT	operational technology
PMU	phasor measurement unit
PSEG	Public Service Enterprise Group
PUC	public utility commission
PURPA	Public Utility Regulation Policy Act
PV	photovoltaic
QER	Quadrennial Energy Review
R&D	research and development
RD&D	research, demonstration, and development
RTO	regional transmission organization
RTU	remote terminal unit
RUS	Rural Utility Service
SAIDI	system average interruption duration index
SAIFI	system average interruption frequency index
SCADA	supervisory control and data acquisition
SoCo	Southern Company
T&D	transmission and distribution
UAV	unmanned aerial vehicle